

Produkthandbuch

McAfee ePolicy Orchestrator 5.0.0 – Software

MARKEN

McAfee, das McAfee-Logo, McAfee Active Protection, McAfee AppPrism, McAfee Artemis, McAfee CleanBoot, McAfee DeepSAFE, ePolicy Orchestrator, McAfee ePO, McAfee EMM, McAfee Enterprise Mobility Management, Foundscore, Foundstone, McAfee NetPrism, McAfee Policy Enforcer, Policy Lab, McAfee QuickClean, Safe Eyes, McAfee SECURE, SecureOS, McAfee Shredder, SiteAdvisor, SmartFilter, McAfee Stinger, McAfee Total Protection, TrustedSource, VirusScan, WaveSecure, WormTraq sind Marken oder eingetragene Marken von McAfee, Inc. oder der Tochterunternehmen in den USA und anderen Ländern. Alle anderen Namen und Marken sind Eigentum der jeweiligen Besitzer.

INFORMATIONEN ZUR LIZENZ

Lizenzvereinbarung

HINWEIS FÜR ALLE BENUTZER: LESEN SIE DEN LIZENZVERTRAG FÜR DIE VON IHNEN ERWORBENE SOFTWARE SORGFÄLTIG DURCH. ER ENTHÄLT DIE ALLGEMEINEN BESTIMMUNGEN UND BEDINGUNGEN FÜR DIE VERWENDUNG DER LIZENZIERTEN SOFTWARE. WENN SIE NICHT WISSEN, WELCHEN SOFTWARE-LIZENZTYP SIE ERWORBEN HABEN, SCHLAGEN SIE IN DEN UNTERLAGEN ZUM KAUF UND WEITEREN UNTERLAGEN BEZÜGLICH DER LIZENZGEWÄHRUNG ODER DEN BESTELLUNTERLAGEN NACH, DIE SIE ZUSAMMEN MIT DEM SOFTWAREPAKET ODER SEPARAT (ALS BROSCHÜRE, DATEI AUF DER PRODUKT-CD ODER ALS DATEI, DIE AUF DER WEBSITE VERFÜGBAR IST, VON DER SIE AUCH DAS SOFTWAREPAKET HERUNTERGELADEN HABEN) ERHALTEN HABEN. WENN SIE MIT DEN IN DIESER VEREINBARUNG AUFGEFÜHRTEN BESTIMMUNGEN NICHT EINVERSTANDEN SIND, UNTERLASSEN SIE DIE INSTALLATION DER SOFTWARE. SOFERN MÖGLICH, GEBEN SIE DAS PRODUKT AN MCAFEE ODER IHREN HÄNDLER BEI VOLLER RÜCKERSTATTUNG DES KAUFPREISES ZURÜCK.

Inhaltsverzeichnis

Einführung in McAfee ePolicy Orchestrator

Einrichten des ePolicy Orchestrator-Servers

Überwachung und Berichterstellung zum Netzwerk-Sicherheitsstatus

Einführung in McAfee ePolicy Orchestrator

In diesem Kapitel lernen Sie die Komponenten von ePolicy Orchestrator kennen und erfahren, wie diese für mehr Sicherheit der Systeme in einem Netzwerk zusammenarbeiten.

1 Schutz Ihrer Netzwerke mithilfe von ePolicy Orchestrator

ePolicy Orchestrator ist eine zentrale Komponente der McAfee-Sicherheits-Management-Plattform, die eine einheitliche Verwaltung von Endgeräte-, Netzwerk- und Datensicherheit bietet. Mit den Automatisierungsfunktionen von ePolicy Orchestrator und dank einer durchgängigen Netzwerktransparenz verkürzt sie Reaktionszeiten, verbessert den Schutz und vereinfacht die Risiko- sowie Sicherheitsverwaltung.

Inhalt

Vorteile von ePolicy Orchestrator

ePolicy Orchestrator ist eine skalierbare, erweiterbare Verwaltungsplattform, die eine zentralisierte Richtlinienverwaltung und -erzwingung für Sicherheitsprodukte und Systeme, auf denen diese installiert sind, ermöglicht. Die Software bietet außerdem umfassende Funktionen zur Berichterstellung und zentralen Produktausbringung.

Mithilfe eines ePolicy Orchestrator-Servers können Sie Folgendes durchführen:

- Sie können Sicherheitsprodukte, Patches und Service Packs auf Systemen in einem Netzwerk ausbringen.
- Sie können die auf den Systemen installierten Host- und Netzwerksicherheitsprodukte durch Erzwingung von Sicherheitsrichtlinien und mithilfe von Client-Tasks und Server-Tasks verwalten.
- Sie können die von Ihrer Sicherheits-Software benötigten Virusdefinitionsdateien (DAT-Dateien), Virenschutz-Module und anderen Sicherheitsinhalte aktualisieren, um die Sicherheit Ihrer verwalteten Systeme zu gewährleisten.

Komponenten und ihre Funktion

ePolicy Orchestrator besteht aus den folgenden Komponenten.

- McAfee ePO-Server – Der Mittelpunkt einer verwalteten Umgebung. Der Server liefert Sicherheitsrichtlinien und Tasks, steuert Aktualisierungen und verarbeitet Ereignisse für alle verwalteten Systeme.
- Datenbank – Die zentrale Speicherkomponente für alle von ePolicy Orchestrator erstellten und verwendeten Daten. Sie können je nach den Anforderungen Ihrer Organisation selbst auswählen, ob sich die Datenbank auf dem McAfee ePO-Server oder auf einem separaten System befinden soll.

- McAfee Agent – Ein Hilfsmittel zum Übertragen von Informationen und zum Erzwingen von Richtlinien zwischen dem ePolicy Orchestrator-Server und den einzelnen verwalteten Systemen. Der Agent ruft für jedes verwaltete System Aktualisierungen ab, stellt die Implementierung von Tasks sicher, erzwingt Richtlinien und leitet Ereignisse weiter. Die Daten überträgt er über einen sicheren Datenkanal an den Server. Ein McAfee Agent kann auch als ein SuperAgent konfiguriert werden.
- Master-Repository – Der zentrale Speicherort für alle McAfee-Aktualisierungen und -Signaturen auf dem ePolicy Orchestrator-Server. Das Master-Repository ruft vom Benutzer angegebene Aktualisierungen und Signaturen von McAfee oder von benutzerdefinierten Quellsites ab.
- Verteilte Repositories – Strategisch günstig über die gesamte Umgebung verteilte Zugriffspunkte, aus denen Agenten Signaturen, Produktaktualisierungen und Produktinstallationen bei minimaler Belastung des Netzwerks empfangen können. Je nach Konfiguration Ihres Netzwerks können Sie verteilte Repositories für SuperAgent oder für die HTTP-, FTP- bzw. UNC-Freigabe einrichten.
- Remote Agentensteuerungen – Ein Server, der an verschiedenen Stellen im Netzwerk installiert werden kann, um beim Verwalten der Agenten-Kommunikation, beim Lastausgleich und bei Produktaktualisierungen zu helfen. Remote Agentensteuerungen bestehen aus einem Apache-Server und einer Ereignisanalyse. Mit ihrer Hilfe können die Anforderungen großer oder komplexer Netzwerkinfrastrukturen besser bewältigt werden, da sie eine bessere Kontrolle über die Agent-zu-Server-Kommunikation ermöglichen.
- Registrierte Server – Werden verwendet, um andere Server bei Ihrem ePolicy Orchestrator-Server zu registrieren. Zu den Typen registrierter Server gehören:
  - LDAP-Server – Wird für Richtlinienzuweisungsregeln sowie zum Aktivieren der automatischen Benutzerkontenerstellung verwendet.
  - SNMP-Server – Wird zum Empfangen eines SNMP-Traps verwendet. Damit ePolicy Orchestrator weiß, wohin der Trap gesendet werden soll, müssen Sie die Informationen für den SNMP-Server hinzufügen.
  - Datenbank-Server – Wird verwendet, um die Tools zur erweiterten Berichterstellung aus dem Lieferumfang von ePolicy Orchestrator weiter auszubauen.
  - Ticket-Server – Bevor Tickets Problemen zugeordnet werden können, muss ein registrierter Ticket-Server konfiguriert werden. Das System, auf dem die Ticket-Erweiterung ausgeführt wird, muss die Adresse des Service Desk-Systems auflösen können.



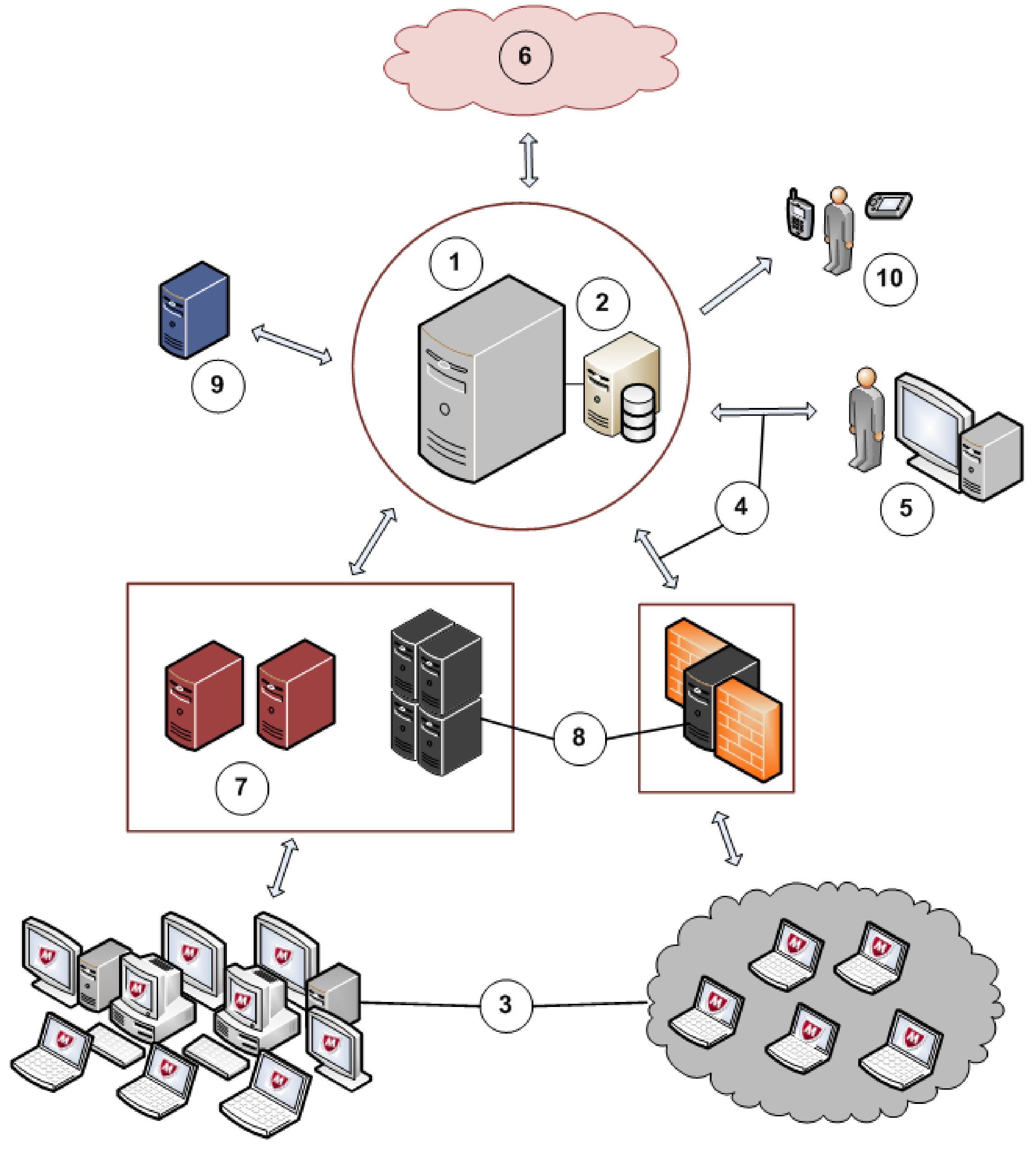
Je nach den Anforderungen Ihres Unternehmens und der Komplexität Ihres Netzwerks sind möglicherweise nicht alle diese Komponenten erforderlich.

Funktionsweise der Software

McAfee ePO ist äußerst flexibel. Es kann auf verschiedene Weisen eingerichtet werden, um Ihre Anforderungen zu erfüllen.

Die Software folgt dem klassischen Client-Server-Modell, bei dem ein Client-System (System) sich für Anweisungen an den Server wendet. Um diesen Kontakt zum Server zu ermöglichen, wird auf jedem System im Netzwerk ein McAfee Agent ausgebracht. Sobald ein Agent auf einem System ausgebracht ist, kann das System vom ePolicy Orchestrator-Server verwaltet werden. Das Bindeglied, das sämtliche Komponenten von ePolicy Orchestrator miteinander verknüpft, ist die sichere Kommunikation zwischen

dem Server und den verwalteten Systemen. In der folgenden Abbildung wird anhand eines Beispiels gezeigt, wie der ePolicy Orchestrator-Server und seine Komponenten in einer sicheren Netzwerkumgebung miteinander interagieren.



1 Der ePolicy Orchestrator-Server ist mit dem McAfee-Aktualisierungs-Server verbunden, um aktuelle Sicherheitsinhalte abzurufen.

2 In der ePolicy Orchestrator-Datenbank werden sämtliche Daten zu den im Netzwerk verwalteten Systemen gespeichert. Dazu gehören:

- Systemeigenschaften
- Richtlinieninformationen
- Verzeichnisstruktur
- Alle sonstigen relevanten Daten, die der Server benötigt, um die Systeme auf dem aktuellen Stand zu halten

3. Auf den Systemen sind McAfee Agents ausgebracht, um die folgenden Punkte zu ermöglichen:
   - Richtlinienerzwingung
   - Produktausbringungen und -aktualisierungen
   - Berichterstellung zu den verwalteten Systemen
4. In regelmäßigen Abständen erfolgt zwischen den Systemen und dem Server eine sichere Agenten-Server-Kommunikation (ASSC). Wenn im Netzwerk remote Agentensteuerungen installiert sind, kommunizieren die Agenten über die ihnen zugewiesenen Agentensteuerungen mit dem Server.
5. Benutzer melden sich bei der ePolicy Orchestrator-Konsole an, um Sicherheitsverwaltungsaufgaben durchzuführen (z. B. Ausführen von Abfragen, um Berichte zum Sicherheitsstatus zu erstellen, oder Arbeiten mit den Sicherheitsrichtlinien von verwalteten Produkten).
6. Auf dem McAfee-Aktualisierungs-Server befinden sich die aktuellsten Sicherheitsinhalte, von wo sie ePolicy Orchestrator in geplanten Abständen abrufen kann.
7. Im gesamten Netzwerk platzierte verteilte Repositories dienen als lokale Hosts für Sicherheitsinhalte, damit Agenten ihre Aktualisierungen schneller erhalten.
8. Remote Agentensteuerungen helfen beim Skalieren des Netzwerks, damit mit einem einzigen ePolicy Orchestrator-Server mehr Agenten verwaltet werden können.
9. Ticket-Server sind mit dem ePolicy Orchestrator-Server verbunden, um beim Verwalten von Problemen und Tickets zu helfen.
10. Benachrichtigungen vom Typ "Automatische Antwort" werden an Sicherheitsadministratoren gesendet, um sie beim Auftreten bestimmter Ereignisse zu informieren.

2 Verwenden der ePolicy Orchestrator-Oberfläche

Melden Sie sich bei der Benutzeroberfläche von ePolicy Orchestrator an, um den McAfee ePO-Server zu konfigurieren sowie die Sicherheit Ihres Netzwerks zu verwalten und zu überwachen.

Inhalt

Navigieren in der Benutzeroberfläche

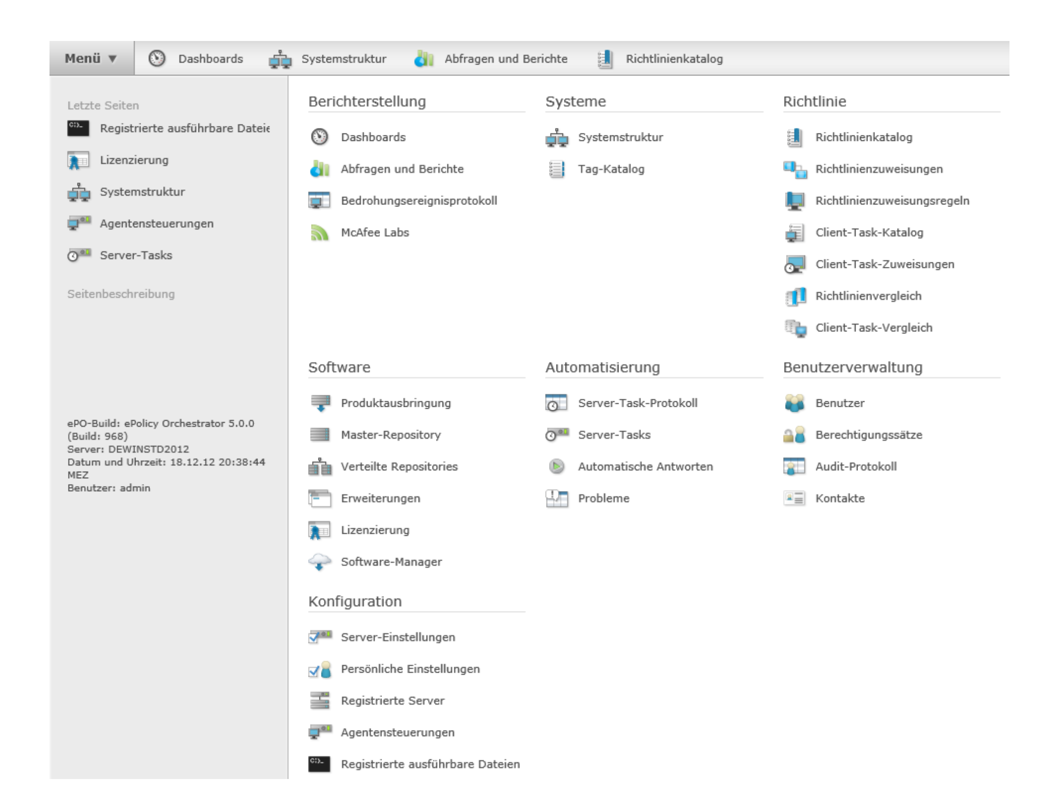
Die Benutzeroberfläche von ePolicy Orchestrator wurde nach einem menübasierten Navigationsmodell mit einer anpassbaren Favoritenleiste gestaltet, sodass Sie schnell zu den gewünschten Bereichen gelangen.

Die Hauptmenüs entsprechen den wichtigsten Funktionen Ihres ePolicy Orchestrator-Server. Wenn neue verwaltete Produkte zum Server hinzugefügt werden, werden die zugehörigen Seiten entweder einer vorhandenen Kategorie zugeordnet oder eine neue Kategorie wird im Menü erstellt.

Navigieren in ePolicy Orchestrator mithilfe des Menüs

Mit dem ePolicy Orchestrator-**Menü** können Sie in der Benutzeroberfläche von ePolicy Orchestrator navigieren.

Das **Menü** besteht aus Kategorien, in denen die verschiedenen Funktionen und Merkmale eines McAfee ePO-Servers enthalten sind. Jede Kategorie enthält eine Liste der Seiten für die wichtigsten Funktionen, die mit einem eindeutigen Symbol versehen sind. Wählen Sie eine Kategorie im **Menü** aus, um die Hauptseiten anzuzeigen, die es zu der entsprechenden Funktion gibt.



Anpassen der Navigationsleiste

Die Navigationsleiste kann angepasst werden, um einen schnellen Zugriff auf die am häufigsten genutzten Funktionen und Merkmale zu ermöglichen.

Sie können selbst entscheiden, welche Symbole in der Navigationsleiste angezeigt werden, indem Sie beliebige Menüelemente in die Navigationsleiste ziehen oder daraus wieder entfernen.

Auf Systemen mit einer Bildschirmauflösung von 1024 x 768 Pixeln können in der Navigationsleiste bis zu sechs Symbole angezeigt werden. Wenn Sie mehr als sechs Symbole in der Navigationsleiste platzieren, wird auf der rechten Seite der Leiste ein Einblendmenü erstellt. Klicken Sie auf das Pfeilsymbol, um auf die Menüelemente zuzugreifen, die nicht in der Navigationsleiste angezeigt werden. Die in der Navigationsleiste angezeigten Symbole werden als Einstellungen des jeweiligen Benutzers gespeichert. Jedem Benutzer wird also unabhängig von der Konsole, an der er sich anmeldet, seine angepasste Navigationsleiste angezeigt.

Server-Einstellungskategorien

In diesem Abschnitt werden die Kategorien der Server-Einstellungen beschrieben, die in ePolicy Orchestrator standardmäßig verfügbar sind.

Beim Einchecken weiterer Software in McAfee ePO-Server werden produktspezifische Server-Einstellungen zur Liste der Server-Einstellungskategorien hinzugefügt. Informationen zu produktspezifischen Server-Einstellungen finden Sie in der zugehörigen Produktdokumentation. Server-Einstellungen können Sie auf der Seite **Server-Einstellungen** im Abschnitt **Konfiguration** der Benutzeroberfläche von ePolicy Orchestrator ändern.

Tabelle 2-1 Kategorien von standardmäßigen Server-Einstellungen und deren Beschreibungen

Server-Einstellungskategorie	Beschreibung
Active Directory-Gruppen	Gibt für jede Domänen den zu verwendenden LDAP-Server an.
Active Directory-Benutzeranmeldung	Gibt an, ob Mitglieder von zugeordneten Active Directory-Gruppen (AD) sich mit ihren AD-Anmeldeinformationen beim Server anmelden können, sobald die Funktion **Active Directory-Benutzeranmeldung** vollständig konfiguriert ist.
Anmeldeinformationen für Agenten-Ausbringung	Gibt an, ob Benutzer die Anmeldeinformationen für die Agenten-Ausbringung in den Cache ablegen dürfen.
Zertifikatbasierte Authentifizierung	Gibt an, ob die zertifikatbasierte Authentifizierung aktiviert ist, sowie die erforderlichen Einstellungen und Konfigurationen für das verwendete Zertifizierungsstellen-Zertifikat.
Dashboards	Gibt das standardmäßig aktive Dashboard an, das dem Konto eines neues Benutzers zum Zeitpunkt der Erstellung zugewiesen wird, sowie die standardmäßige Aktualisierungsrate (5 Minuten) für Dashboard-Monitore.
Wiederherstellung nach Systemausfall	Legt die Passphrase für die Schlüsselspeicherverschlüsselung zur Wiederherstellung nach einem Systemausfall fest und aktiviert sie.
E-Mail-Server	Gibt den E-Mail-Server an, über den ePolicy Orchestrator E-Mail-Nachrichten sendet.
Ereignisfilterung	Legt fest, welche Ereignisse vom Agenten weitergeleitet werden.
Ereignisbenachrichtigungen	Gibt das Intervall an, in dem ePolicy Orchestrator-Benachrichtungsereignisse an automatische Antworten gesendet werden sollen.
Globale Aktualisierung	Gibt an, ob und wie die globale Aktualisierung aktiviert ist.
Lizenzschlüssel	Gibt den Lizenzschlüssel an, mit dem diese ePolicy Orchestrator-Software registriert wurde.
Anmeldenachricht	Gibt die benutzerdefinierte Anmeldenachricht (falls vorhanden) an, die Benutzern angezeigt wird, wenn sie zum Anmeldebildschirm der ePolicy Orchestrator-Konsole wechseln.
Richtlinienwartung	Gibt an, ob Richtlinien für nicht unterstützte Produkte ein- oder ausgeblendet werden. Dies ist nur dann erforderlich, wenn ePolicy Orchestrator aktualisiert wird.
Ports	Gibt die Ports an, über die der Server mit Agenten und der Datenbank kommuniziert.
Drucken und exportieren	Gibt an, wie Informationen in andere Formate exportiert werden, und welche Vorlage bei PDF-Exporten verwendet wird. Außerdem gibt diese Einstellung den Standardspeicherort an, in dem die exportierten Dateien gespeichert werden.
Produktkompatibilitätsliste	Gibt an, ob die Produktkompatibilitätsliste automatisch heruntergeladen wird, und zeigt nicht kompatible Produkterweiterungen an.
Product Improvement Program	Gibt an, ob McAfee proaktiv und in regelmäßigen Abständen Daten auf den vom McAfee ePO-Server verwalteten Client-Systemen erfassen darf.
Proxyeinstellungen	Gibt den Typ der für Ihren McAfee ePO-Server konfigurierten Proxyeinstellungen an.

Tabelle 2-1 Kategorien von standardmäßigen Server-Einstellungen und deren Beschreibungen *(Fortsetzung)*

Server-Einstellungskategorie	Beschreibung
Sicherheitsschlüssel	Gibt die ASSC-Schlüssel (Agent-Server Secure Communication, sichere Agenten-Server-Kommunikation) und Repository-Schlüssel an und verwaltet sie.
Server-Zertifikat	Gibt das Server-Zertifikat an, das von dem McAfee ePO-Server bei der HTTPS-Kommunikation mit Browsern verwendet wird.
Software-Test	Gibt die erforderlichen Informationen an, die für das Einchecken und Ausbringen von Test-Software im Software-Manager bereitgestellt wurden.
Quellsites	Gibt die Quellsites an, zu denen der Server für Aktualisierungen eine Verbindung herstellt, sowie die Sites, die als alternative Sites verwendet werden sollen.
Systemdetaileinstellungen	Gibt an, welche Abfragen und Systemeigenschaften auf der Seite **Systemdetails** für verwaltete Systeme angezeigt werden.
Systemstruktursortierung	Gibt an, ob und wie die Systemstruktursortierung in der Umgebung aktiviert ist.
Benutzersitzung	Gibt an, wie lange ein Benutzer inaktiv sein darf, bevor er vom System abgemeldet wird.

Arbeiten mit Listen und Tabellen

Tabellendaten können Sie mithilfe der Such- und Filterfunktionen von ePolicy Orchestrator sortieren.

Filtern einer Liste

Die Listen in der Benutzeroberfläche von ePolicy Orchestrator enthalten viele Informationen. Mithilfe voreingestellter oder benutzerdefinierter Filter sowie der Funktion zur Zeilenauswahl können Sie eine Liste auf relevante Elemente beschränken.



Nicht alle Filter sind bei jeder Liste verfügbar.

- Wählen Sie in der Leiste oberhalb der Liste den voreingestellten oder benutzerdefinierten Filter aus, mit dem die Liste gefiltert werden soll.

  Es werden nur Einträge angezeigt, die den Filterkriterien entsprechen.

- Aktivieren Sie die Kontrollkästchen neben den Listeneinträgen, auf die Sie sich konzentrieren möchten, und aktivieren Sie dann das Kontrollkästchen **Ausgewählte Zeilen anzeigen**.

  Es werden nur die ausgewählten Zeilen angezeigt.

Suchen nach bestimmten Listeneinträgen

Verwenden Sie den Filter **Schnellsuche**, um Einträge in einer längeren Liste schneller zu finden.



Namen von Standardabfragen können übersetzt vorliegen. Wenn Sie mit Benutzern aus anderen Ländern kommunizieren, sollten Sie daran denken, dass Abfragenamen anders lauten könnten.

Vorgehensweise

Definitionen zu Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

1. Geben Sie Ihren Suchbegriff in das Feld **Schnellsuche** ein.
2. Klicken Sie auf **Übernehmen**.

Es werden nur die Elemente angezeigt, die die im Feld **Schnellsuche** eingegebenen Begriffe enthalten.



Wenn Sie die Filterung wieder aufheben und alle Listeneinträge anzeigen möchten, klicken Sie auf **Löschen**.

Aktivieren der Kontrollkästchen von Tabellenzeilen

In der Benutzeroberfläche von ePolicy Orchestrator können Sie mithilfe spezieller Methoden und Tastenkombinationen die Tabellenzeilen auswählen. Dabei aktivieren Sie die Kontrollkästchen der einzelnen Tabellenzeilen, indem Sie entweder wie üblich oder mit gedrückter **UMSCHALTTASTE** auf das Kästchen **klicken**.

Auf einigen Ausgabeseiten in der ePolicy Orchestrator-Benutzeroberfläche wird neben jeder Zeile in einer Tabelle ein Kontrollkästchen angezeigt. Mithilfe dieser Kontrollkästchen können Sie einzelne, mehrere oder alle Zeilen in der Tabelle auswählen.

In der folgenden Tabelle sind die Tastenkombinationen aufgeführt, mit denen Sie die Kontrollkästchen von Tabellenzeilen auswählen können.

Auswahl	Aktion	Ergebnis
Einzelne Zeilen	Klicken Sie auf die einzelnen Zeilen.	Die einzelnen Zeilen werden unabhängig voneinander ausgewählt.
Eine Gruppe von Zeilen	Klicken Sie auf das Kontrollkästchen der ersten gewünschten Zeile, und **klicken** Sie dann mit gedrückter **UMSCHALTTASTE** auf das letzte gewünschte Kontrollkästchen.	Es wird eine Gruppe von Zeilen ausgewählt, die von der ersten bis zur letzten ausgewählten Zeile reicht. Wenn mittels **Mausklick** bei gedrückter **UMSCHALTTASTE** mehr als 1.500 Zeilen gleichzeitig ausgewählt sind, kann dies zu einer zu hohen CPU-Auslastung führen und eine Fehlermeldung bezüglich eines Skriptfehlers auslösen.
Alle Zeilen	Klicken Sie auf das Kontrollkästchen ganz oben in der Tabellenüberschrift.	Es werden sämtliche Zeilen in der Tabelle ausgewählt.

Einrichten des ePolicy Orchestrator-Servers

Das Einrichten des ePolicy Orchestrator-Servers ist der erste Schritt zum Verwalten Ihrer Netzwerksicherheit.

3 Planen der ePolicy Orchestrator-Konfiguration

Damit Sie Ihren ePolicy Orchestrator-Server effizient nutzen können, müssen Sie über einen umfassenden Plan für Ihre Umgebung verfügen.

Wie Sie Ihre Server-Infrastruktur einrichten und wie umfangreich die durchzuführenden Konfigurationsarbeiten sind, hängt von den jeweiligen Gegebenheiten Ihrer Netzwerkumgebung ab. Je sorgfältiger Sie diese Punkte im Voraus überdenken, desto schneller ist alles eingerichtet und funktionsbereit.

Inhalt

Erwägungen zur Skalierbarkeit

Wie Sie Ihre Skalierbarkeit verwalten, hängt davon ab, ob Sie mehrere ePolicy Orchestrator-Server, mehrere remote Agentensteuerungen oder beide verwenden.

Mit ePolicy Orchestrator können Sie Ihr Netzwerk vertikal oder horizontal skalieren.

- *Vertikale Skalierbarkeit* – Erfolgt durch Hinzufügen von und ein Upgrade auf größere, schnellere Hardware zum Verwalten immer umfangreicherer Ausbringungen. Die vertikale Skalierung der ePolicy Orchestrator-Server-Infrastruktur wird durch ein Upgrade der Server-Hardware und durch Verwenden mehrerer ePolicy Orchestrator-Server im Netzwerk erreicht, von denen jeder über eine eigene Datenbank verfügt.
- *Horizontale Skalierbarkeit* – Hierbei wird die Größe der Ausbringung gesteigert, die von einem einzigen ePolicy Orchestrator-Server verwaltet werden kann. Erreicht wird dies durch Installation mehrerer remoter Agentensteuerungen, die sich jeweils bei einer einzigen Datenbank melden.

Verwenden mehrerer McAfee ePO-Server

Je nach Größe und Aufbau einer Organisation kann der Einsatz mehrerer McAfee ePO-Server erforderlich sein.

Der Einsatz mehrerer Server kann in Szenarien wie den folgenden erforderlich sein:

- Für jede Abteilung in Ihrem Unternehmen soll eine eigene Datenbank unterhalten werden.
- Es werden separate IT-Infrastrukturen, administrative Gruppen oder Testumgebungen benötigt.
- Das Unternehmen ist über mehrere geographische Standorte verteilt und nutzt eine Netzwerkverbindung mit relativ geringer Bandbreite, z. B. WAN, VPN oder andere langsamere Verbindungen, die meist zwischen remoten Standorten eingesetzt werden. Weitere Informationen zu Anforderungen bezüglich der Bandbreite finden Sie im *McAfee ePolicy Orchestrator-Handbuch zur Hardware-Dimensionierung und Bandbreitennutzung*.

Beim Einsatz mehrerer Server in einem Netzwerk ist es erforderlich, für jeden Server eine eigene Datenbank zu unterhalten. Die in den einzelnen Servern befindlichen Informationen können Sie auf dem McAfee ePO-Haupt-Server und der Hauptdatenbank zusammenfassen.

Verwenden mehrerer remoter Agentensteuerungen

Durch den Einsatz mehrerer remoter Agentensteuerungen können Sie größere Ausbringungen verwalten, ohne dass dafür zusätzliche McAfee ePO-Server zur Umgebung hinzugefügt werden müssen.

Die Agentensteuerung ist die Komponente des Servers, die für die Verwaltung von Agenten-Anforderungen zuständig ist. Jede McAfee ePO-Server-Installation verfügt standardmäßig über eine Agentensteuerung. Der Einsatz mehrerer remoter Agentensteuerungen kann in Szenarien wie den folgenden erforderlich sein:

- Sie möchten, dass Agenten zwischen mehreren physischen Geräten wählen können, damit sie auch im Falle eines nicht verfügbaren Anwendungs-Servers noch in der Lage sind, sich zu melden und Richtlinien-, Task- und Produktaktualisierungen abzurufen. Und Sie möchten dies erreichen, ohne dazu einen Cluster Ihres ePolicy Orchestrator-Servers zu erstellen.
- Die vorhandene ePolicy Orchestrator-Infrastruktur muss erweitert werden, um mehr Agenten, weitere Produkte oder eine aus kürzeren Agent-zu-Server-Kommunikationsintervallen resultierende höhere Arbeitslast zu bewältigen.
- Sie möchten mit Ihrem ePolicy Orchestrator-Server voneinander getrennte Netzwerksegmente verwalten, z. B. Systeme, die Network Address Translation (NAT) verwenden, oder sich in einem externen Netzwerk befinden.



Dies funktioniert, solange die Agentensteuerung über eine Verbindung mit hoher Bandbreite zur ePolicy Orchestrator-Datenbank verfügt.

Durch den Einsatz mehrerer Agentensteuerungen kann die Skalierbarkeit erhöht und die Komplexität bei der Verwaltung umfangreicherer Ausbringungen verringert werden. Da Agentensteuerungen jedoch eine schnelle Netzwerkverbindung benötigen, gibt es Szenarien, für die sie eher nicht geeignet sind, wie zum Beispiel:

- Als Ersatz für verteilte Repositories. Verteilte Repositories sind lokale Dateifreigaben, mit denen der bei der Agenten-Kommunikation anfallende Datenverkehr niedrig gehalten werden soll. Auch wenn in Agentensteuerungen eine Repository-Funktion integriert ist, müssen Sie permanent mit der ePolicy Orchestrator-Datenbank kommunizieren und belegen daher einen deutlich größeren Anteil an Bandbreite.
- Zur Verbesserung der Repository-Replizierung über eine WAN-Verbindung. Der bei der Repository-Replizierung erforderliche permanente Kommunikationsfluss zur Datenbank kann die gesamte Bandbreite der WAN-Verbindung in Anspruch nehmen.
- Zum Verbinden eines abgetrennten Netzwerksegments, aus dem nur begrenzte oder unregelmäßige Verbindungen zur ePolicy Orchestrator-Datenbank erfolgen.

Internetprotokolle in einer verwalteten Umgebung

ePolicy Orchestrator ist mit beiden IP-Versionen (d. h. IPv4 und IPv6) kompatibel.

ePolicy Orchestrator-Server arbeiten in drei verschiedenen Modi:

- Nur IPv4 – Unterstützt nur das IPv4-Adressformat.
- Nur IPv6 – Unterstützt nur das IPv6-Adressformat.
- Gemischter Modus – Unterstützt sowohl das IPv4- als auch das IPv6-Adressformat.

In welchem Modus ein ePolicy Orchestrator-Server arbeitet, hängt von der Netzwerkkonfiguration ab. Wenn das Netzwerk zum Beispiel so konfiguriert ist, dass nur IPv4-Adressen verwendet werden, arbeitet der Server im Modus "Nur IPv4". Wenn das Netzwerk dagegen so konfiguriert ist, dass sowohl IPv4- als auch IPv6-Adressen verwendet werden, arbeitet der Server im gemischten Modus.

Solange IPv6 nicht installiert und aktiviert ist, reagiert der ePolicy Orchestrator-Server nur auf IPv4-Adressen. Wenn IPv6 aktiviert ist, arbeitet der Server in dem Modus, in dem er konfiguriert ist.

Wenn der McAfee ePO-Server per IPv6 mit einer Agentensteuerung oder einem Rogue System Sensor kommuniziert, werden adressrelevante Eigenschaften (z. B. IP-Adresse, Subnetzadresse und Subnetzmaske) im IPv6-Format gemeldet. Bei der Übertragung zwischen Client und ePolicy Orchestrator-Server oder bei der Anzeige in der Benutzeroberfläche oder Protokolldatei werden IPv6-relevante Eigenschaften in der erweiterten Form angezeigt und in Klammern gesetzt.

So wird zum Beispiel 3FFE:85B:1F1F::A9:1234 als [3FFE:085B:1F1F:0000:0000:0000:00A9:1234] angezeigt.

Beim Festlegen einer IPv6-Adresse für FTP- oder HTTP-Quellen sind keine Änderungen an der Adresse erforderlich. Beim Festlegen einer literalen IPv6-Adresse für eine UNC-Quelle müssen Sie jedoch das Microsoft-Format für literale IPv6-Adressen verwenden. Weitere Informationen dazu finden Sie in der Microsoft-Dokumentation.

4 Einrichten des McAfee ePO-Servers

Beschleunigen Sie die Einsatzbereitschaft der Software, indem Sie die grundlegenden Funktionen des McAfee ePO-Servers konfigurieren.

Inhalt

Überblick über die Server-Konfiguration

Wie der ePolicy Orchestrator-Server eingerichtet wird, hängt von den jeweiligen Anforderungen einer Umgebung ab.

Dieser Überblick konzentriert sich auf die wichtigsten Einrichtungs- und Konfigurationsschritte für den ePolicy Orchestrator-Server. Jeder Schritt stellt ein Kapitel oder einen Abschnitt in diesem Produkthandbuch dar, in dem Sie ausführliche Informationen über die Merkmale und Funktionen der Software sowie die Aufgaben finden, mit deren Hilfe diese Merkmale und Funktionen implementiert und verwendet werden.



Je nach der Größe und Komplexität Ihres Netzwerks müssen Sie nicht alle verfügbaren Funktionen konfigurieren.

Prozessüberblick

Diese Anleitung ist ein allgemeiner Überblick über den Konfigurationsvorgang für einen Server. Viele Punkte stehen für bestimmte Funktionsgruppen oder Funktionsbereiche von ePolicy Orchestrator:

1. **Konfigurieren grundlegender Funktionen** – ePolicy Orchestrator enthält grundlegende Funktionen, die Sie konfigurieren müssen, damit Ihr Server ordnungsgemäß funktioniert. Mithilfe des Tools **Geführte Konfiguration** können Sie die grundlegenden Funktionen Ihres McAfee ePO-Servers konfigurieren.
2. **Konfigurieren allgemeiner Server-Einstellungen** – Server-Einstellungen aus dieser Gruppe betreffen Funktionen, die Sie für den ordnungsgemäßen Betrieb Ihres Servers nicht ändern müssen, mit denen Sie jedoch einige Verhaltensweisen Ihres Servers anpassen können.
3. **Erstellen von Benutzerkonten** – Mithilfe von Benutzerkonten können Benutzer auf den Server zugreifen.

4. **Konfigurieren von Berechtigungssätzen** – Berechtigungssätze gewähren Rechte und Zugriff auf Funktionen von ePolicy Orchestrator.
5. **Konfigurieren erweiterter Server-Einstellungen und -Funktionen** – Der ePolicy Orchestrator-Server verfügt über erweiterte Funktionen und Merkmale, mit denen Sie die Verwaltung Ihrer Netzwerksicherheit automatisieren können.
6. **Einrichten zusätzlicher Komponenten** – Für die Verwendung vieler erweiterter Funktionen von ePolicy Orchestrator sind zusätzliche Komponenten wie verteilte Repositories, registrierte Server und Agentensteuerungen erforderlich.

Grundlegende Funktionen

Einige Funktionen des McAfee ePO-Servers sind für seine Funktionsfähigkeit von grundlegender Bedeutung und müssen entsprechend konfiguriert werden, bevor Sie Sicherheits-Software auf den Systemen in Ihrem Netzwerk ausbringen und verwalten können.

Zu den grundlegenden Funktionen des McAfee ePO-Servers gehören die folgenden Elemente:

- Der Software-Manager – Hiermit können Sie neue und aktualisierte Sicherheits-Software von der Konsole aus in den ePolicy Orchestrator-Server und in das Master-Repository einchecken.
- Die Systemstruktur – Sie enthält sämtliche von Ihrem ePolicy Orchestrator-Server verwalteten Systeme.
- Der Richtlinienkatalog – Hier konfigurieren Sie die Sicherheitsrichtlinien, mit denen die auf Ihren verwalteten Systemen ausgebrachte Sicherheits-Software gesteuert wird.
- Der Client-Task-Katalog – Hier können Sie Client-Tasks erstellen, zuweisen und planen, um Tasks zu automatisieren, die auf den verwalteten Systemen ausgeführt werden.
- Der McAfee Agent – Diese Komponente ermöglicht die Verwaltung eines Systems im Netzwerk. Sobald der Agent ausgebracht ist, übermittelt er den Status und alle zugehörigen Daten zum und aus dem Server und dem verwalteten System. Er stellt das Hilfsmittel dar, über das die Sicherheits-Software ausgebracht, Richtlinien erzwungen und Tasks zugewiesen werden.



McAfee Agent ist ein unabhängiges Software-Produkt, das der ePolicy Orchestrator-Server benötigt, um Systeme im Netzwerk zu verwalten. Er wird bei der Erstinstallation von McAfee ePO automatisch in das Master-Repository eingecheckt.

Diese Version der Software enthält auch das ePolicy Orchestrator-Tool zur geführten Konfiguration. Mithilfe dieses Tools können Sie die grundlegenden Funktionen leichter konfigurieren und sich mit der Benutzeroberfläche von ePolicy Orchestrator vertraut machen. Die geführte Konfiguration hilft beim Durchführen der erforderlichen Schritte für die folgenden Aufgaben:

1. Einchecken von McAfee-Sicherheits-Software in Ihr Master-Repository, damit sie auf den Systemen in Ihrem Netzwerk ausgebracht werden kann
2. Hinzufügen der Systeme zur Systemstruktur von ePolicy Orchestrator, damit Sie sie verwalten können
3. Erstellen und Zuweisen mindestens einer Sicherheitsrichtlinie, die auf den verwalteten Systemen erzwungen werden soll
4. Planen eines Client-Tasks, der die Sicherheits-Software auf dem aktuellen Stand hält
5. Ausbringen der Sicherheits-Software auf den verwalteten Systemen

Die Verwendung des Tools zur geführten Konfiguration ist nicht obligatorisch. Sie können jeden dieser Schritte auch manuell durchführen. Bei einer manuellen Durchführung wird jedoch empfohlen, dass Sie während des Konfigurationsvorgangs einen ähnlichen Arbeitsablauf einhalten. Unabhängig davon, nach welcher Vorgehensweise Sie diese Funktionen konfigurieren, können Sie die Konfiguration Ihres Servers mithilfe des Tools zur geführten Konfiguration oder direkt auf den einzelnen Seiten im Menü von McAfee ePO ändern und optimieren.

Konfigurieren grundlegender Funktionen

Das Tool **Geführte Konfiguration** führt Sie durch die einzelnen Seiten, auf denen grundlegende Funktionen konfiguriert werden.

Führen Sie jeden der nachfolgend aufgeführten Schritte durch:

- Wählen Sie die Sicherheits-Software aus, die auf Systemen in Ihrem Netzwerk ausgebracht werden soll.
- Wählen Sie die Systeme in Ihrem Netzwerk aus, die Sie mit Ihrem McAfee ePO-Server verwalten möchten, und fügen Sie sie zur Systemstruktur hinzu.
- Konfigurieren Sie eine Default-Richtlinie, die den verwalteten Systemen zugewiesen und dort erzwungen werden soll.
- Planen Sie einen Produktaktualisierungs-Task, um sicherzustellen, dass auf den verwalteten Systemen die neuesten Aktualisierungen installiert sind.
- Bringen Sie die Sicherheits-Software auf den verwalteten Systemen aus.



Sie müssen nicht jeden Schritt abschließen, und Sie können jeden Schritt so oft wie gewünscht erneut ausführen. Es wird jedoch empfohlen, dass Sie dieses Konfigurations-Tool wie einen Assistenten verwenden und die einzelnen Schritte in der richtigen Reihenfolge abschließen. Auf diese Weise können Sie sich mit den einzelnen Seiten in der Benutzeroberfläche vertraut machen, auf denen diese Funktionen gesteuert werden, um in Zukunft auch ohne Konfigurations-Tool auszukommen.

Vorgehensweise

Definitionen zu Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

1. Klicken Sie in der ePolicy Orchestrator-Konsole auf **Menü** | **Berichterstellung** | **Dashboards**, wählen Sie im Dropdown-Menü **Dashboard** den Eintrag **Geführte Konfiguration** aus, und klicken Sie dann auf **Starten**.
2. Lesen Sie die Übersicht und die Anweisungen zur geführten Konfiguration, und klicken Sie dann auf **Starten**.
3. Die Seite **Software-Auswahl** wird geöffnet. So führen Sie diesen Schritt aus:
   a. Klicken Sie unter der Produktkategorie **Nicht eingecheckte Software** auf **Lizenziert** oder **Test**, um die verfügbaren Produkte anzuzeigen.
   b. Wählen Sie in der Tabelle **Software** das Produkt aus, das eingecheckt werden soll. Die Produktbeschreibung und alle verfügbaren Komponenten werden unten in der Tabelle angezeigt.
   c. Klicken Sie auf **Alle einchecken**, um Produkterweiterungen in den ePolicy Orchestrator-Server und Produktpakete in das Master-Repository einzuchecken.
   d. Klicken Sie oben im Bildschirm auf **Weiter**, wenn die Software eingecheckt ist und Sie mit dem nächsten Schritt fortfahren möchten.

4 Die Seite **Systemauswahl** wird geöffnet. So führen Sie diesen Schritt aus:

a Wählen Sie aus, zu welcher Gruppe in der **Systemstruktur** die Systeme hinzugefügt werden sollen. Wenn noch keine benutzerdefinierten Gruppen vorhanden sind, wählen Sie **Eigene Organisation** aus und klicken dann auf **Weiter**. Das Dialogfeld **Hinzufügen der Systeme** wird geöffnet.

b Wählen Sie aus, auf welche Weise Sie die Systeme zur **Systemstruktur** hinzufügen möchten:

Methode	Aktion	Vorgehensweise
AD-Synchronisierung	Synchronisieren Sie den ePolicy Orchestrator-Server mit Ihrem Active Directory-Server oder Domänen-Controller. Wenn in Ihrer Umgebung einer dieser Server vorhanden ist, stellt die Active Directory-Synchronisierung die schnellste Möglichkeit dar, Systeme zur Systemstruktur hinzuzufügen.	1 Wählen Sie im Dialogfeld **AD-Synchronisierung** den gewünschten **Synchronisierungstyp** aus, und geben Sie die entsprechenden Einstellungen an. 2 Klicken Sie auf **Synchronisieren und speichern**, um mit dem nächsten Schritt fortzufahren.
Manuell	Sie können Systeme manuell zur Systemstruktur hinzufügen, indem Sie deren Namen angeben oder eine Liste mit Systemen pro Domäne durchsuchen.	1 Klicken Sie auf der Seite **Neue Systeme** auf **Durchsuchen**, um einzelne Systeme aus einer Domäne hinzuzufügen, und klicken Sie auf **OK**, oder geben Sie im Feld **Zielsysteme** Namen von Systemen an. 2 Klicken Sie auf **Systeme hinzufügen**, um mit dem nächsten Schritt fortzufahren.

5 Die Seite **Richtlinienkonfiguration** wird geöffnet. So führen Sie diesen Schritt aus:

Option	Aktion	Vorgehensweise
Standardeinstellungen verwenden	Verwenden Sie für die Software, die Sie ausbringen möchten, die Richtlinieneinstellung **My Default**, und setzen Sie die Konfiguration fort.	Damit ist dieser Schritt abgeschlossen.
Richtlinie konfigurieren	Geben Sie nun für die einzelnen Software-Produkte, die Sie eingecheckt haben, benutzerdefinierte Richtlinieneinstellungen an.	1 Klicken Sie im Dialogfeld **Richtlinienkonfiguration** auf **OK**. 2 Wählen Sie in der **Produktliste** ein Produkt aus, und klicken Sie auf **My Default**, um die Einstellungen der Default-Richtlinie zu bearbeiten. 3 Klicken Sie auf **Weiter**, um mit dem nächsten Schritt fortzufahren.

6 Die Seite **Software-Aktualisierung** wird geöffnet. So führen Sie diesen Schritt aus:

Option	Aktion	Vorgehensweise
Standardzeitplan erstellen	Erstellen Sie automatisch einen standardmäßigen Client-Produktaktualisierungs-Task, der täglich um 12:00 Uhr ausgeführt wird.	Damit ist dieser Schritt abgeschlossen.
Task-Plan festlegen	Konfigurieren Sie den Zeitplan für Ihren Client-Produktaktualisierungs-Task manuell.	**1** Geben Sie im **Generator für Client-Task-Zuweisungen** ein **Produkt** und einen **Task-Namen** für Ihren Produktaktualisierungs-Task an. Ändern Sie nicht die Auswahl im Feld **Task-Typ**. Als **Task-Typ** muss **Produktaktualisierung** eingestellt sein. **2** Konfigurieren Sie die Optionen **Task-Vererbung sperren** und **Tags**, und klicken Sie dann auf **Weiter**. **3** Geben Sie den Zeitplan für den Aktualisierungs-Task an, und klicken Sie dann auf **Weiter**. **4** Überprüfen Sie die Zusammenfassung, und klicken Sie dann auf **Speichern**.

7. Die Seite **Software-Ausbringung** wird geöffnet. So führen Sie diesen Schritt aus:
   a. Wählen Sie in der **Systemstruktur** aus, auf welchen Systemen die Software ausgebracht werden soll, und klicken Sie dann auf **Weiter**. Das Dialogfeld **Software-Ausbringung** wird geöffnet. Klicken Sie auf **OK**, um den Vorgang fortzusetzen.
   b. Legen Sie die Einstellungen für die McAfee Agent-Ausbringung fest, und klicken Sie dann auf **Ausbringen**.



Wenn Sie diese Aktion zu einem späteren Zeitpunkt durchführen möchten, klicken Sie auf **Agenten-Ausbringung überspringen**. Sie können Ihre andere Sicherheits-Software jedoch erst dann ausbringen, wenn Agenten ausgebracht wurden.

   c. Das Dialogfeld **Software-Ausbringung** wird geöffnet. Wählen Sie die Software-Pakete aus, die Sie auf den verwalteten Systemen ausbringen möchten, und klicken Sie dann auf **Ausbringen**.

Das Dialogfeld **Konfigurationszusammenfassung** wird geöffnet. Die Konfiguration ist abgeschlossen. Klicken Sie auf **Fertig stellen**, um die **Geführte Konfiguration** zu schließen.

Verwenden eines Proxyservers

Wenn in der Netzwerkumgebung ein Proxyserver verwendet wird, müssen Sie die Proxyeinstellungen in den ePolicy Orchestrator-Server-Einstellungen angeben.

Vorgehensweise

Definitionen zu Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

1. Klicken Sie auf **Menü** | **Konfiguration** | **Server-Einstellungen**, wählen Sie in der Liste **Einstellungskategorien** den Eintrag **Proxyeinstellungen** aus, und klicken Sie dann auf **Bearbeiten**.
2. Wählen Sie **Proxyeinstellungen manuell konfigurieren** aus, geben Sie die entsprechenden Konfigurationsinformationen an, die der Proxyserver für die einzelnen Gruppen von Optionen verwendet, und klicken Sie dann auf **Speichern**.

Eingeben Ihres Lizenzschlüssels

Ihr Lizenzschlüssel berechtigt Sie zu einer vollständigen Installation der Software und trägt die lizenzierten ePolicy Orchestrator-Produkte, die Ihr Unternehmen besitzt, in den McAfee-Software-Manager ein.

Ohne Lizenzschlüssel wird die Software im Testmodus ausgeführt. Nach Ablauf des Testzeitraums funktioniert die Software nicht mehr. Einen Lizenzschlüssel können Sie zu jedem beliebigen Zeitpunkt während oder nach Ablauf des Testzeitraums hinzufügen.

Vorgehensweise

Definitionen zu Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

1. Klicken Sie auf **Menü** | **Konfiguration** | **Server-Einstellungen**, wählen Sie in der Liste **Einstellungskategorien** den Eintrag **Lizenzschlüssel** aus, und klicken Sie dann auf **Bearbeiten**.
2. Geben Sie Ihren **Lizenzschlüssel** ein, und klicken Sie auf **Speichern**.

Nach dem Einrichten durchzuführende Aufgaben

Nachdem Sie die wichtigsten Funktionen Ihres McAfee ePO-Servers konfiguriert haben, müssen Sie je nach Bedarf die folgenden nach dem Einrichten durchzuführenden Aufgaben durchführen.

- Erstellen von Benutzerkonten und Berechtigungssätzen
- Konfigurieren einer Active Directory-Benutzeranmeldung
- Konfigurieren von zertifikatbasierter Authentifizierung
- Verwalten von Sicherheitsschlüsseln
- Konfigurieren von Quellsites und alternativen Sites
- Einrichten von Repositories
- Einrichten registrierter Server
- Bestimmen der an den Server weiterzuleitenden Ereignisse
- Konfigurieren von Einstellungen für die Wiederherstellung nach einem Systemausfall

5 Benutzerkonten und Berechtigungssätze

Jedem Benutzerkonto sind ein oder mehrere Berechtigungssätze zugewiesen, die festlegen, welche Aktionen der Benutzer mit der Software durchführen darf.

Inhalt

Benutzerkonten

Mithilfe von Benutzerkonten können Sie steuern, auf welche Inhalte Benutzer zugreifen und wie sie die Software nutzen dürfen. Selbst in der kleinsten ePolicy Orchestrator-Installation muss der Zugriff festgelegt und kontrolliert werden, den Benutzer auf die verschiedenen Teile des Systems haben.

Inhalt

Arten von Benutzerkonten

Es gibt zwei Arten von Benutzern: Administratoren und Benutzer mit eingeschränkten Berechtigungen.

Benutzerkonten können auf verschiedene Weisen erstellt und verwaltet werden. Folgende Möglichkeiten stehen zur Verfügung:

- Sie können Benutzerkonten manuell erstellen und dann jedem Konto einen geeigneten Berechtigungssatz zuweisen.
- Sie können den ePolicy Orchestrator-Server so konfigurieren, dass sich Benutzer mittels Windows-Authentifizierung anmelden können.

Das Zulassen von Benutzeranmeldungen mithilfe von Windows-Anmeldeinformationen ist eine erweiterte Funktion, für die mehrere Einstellungen und Komponenten konfiguriert bzw. eingerichtet werden müssen. Weitere Informationen zu dieser Möglichkeit finden Sie unter *Verwalten von ePolicy Orchestrator-Benutzern mit Active Directory*.

Auch wenn Benutzerkonten und Berechtigungssätze in einer engen Beziehung zueinander stehen, werden sie auf unterschiedliche Weise erstellt und konfiguriert. Weitere Informationen zu Berechtigungssätzen finden Sie unter *Einrichten von Berechtigungssätzen*.

Verwalten von Benutzerkonten

Auf der Seite **Benutzerverwaltung** können Sie Benutzerkonten manuell erstellen, bearbeiten und löschen.



Anstatt ein Konto zu löschen, sollten Sie dessen **Anmeldestatus** auf **Deaktiviert** setzen, bis Sie sicher sind, dass alle mit dem Konto verbundenen wichtigen Informationen nun zu anderen Benutzern verschoben wurden.

Vorgehensweise

Definitionen zu Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

1. Klicken Sie auf **Menü** | **Benutzerverwaltung** | **Benutzer**. Die Seite **Benutzerverwaltung** wird angezeigt.
2. Wählen Sie eine der folgenden Aktionen aus.

Aktion	Vorgehensweise
Erstellen eines Benutzers	Klicken Sie auf **Neuer Benutzer**. Die Seite **Neuer Benutzer** wird angezeigt. 1 Geben Sie einen Benutzernamen ein. 2 Legen Sie fest, ob der Anmeldestatus dieses Kontos aktiviert oder deaktiviert werden soll. Wenn das Konto für eine Person gedacht ist, die noch nicht zu Ihrem Unternehmen gehört, möchten Sie es vielleicht erst einmal deaktivieren. 3 Wählen Sie aus, ob das neue Konto **McAfee ePO-Authentifizierung**, **Windows-Authentifizierung** oder **Zertifikatbasierte Authentifizierung** verwendet, und geben Sie die erforderlichen Anmeldeinformationen an, oder wechseln Sie zu dem Zertifikat, und wählen Sie es aus. 4 Optional können Sie im Textfeld **Anmerkungen** den vollständigen Namen, die E-Mail-Adresse, die Telefonnummer und eine Beschreibung des Benutzers eingeben. 5 Legen Sie fest, ob der Benutzer ein Administrator sein soll, oder wählen Sie für den Benutzer die entsprechenden Berechtigungssätze aus. 6 Klicken Sie auf **Speichern**, um zur Registerkarte **Benutzer** zurückzukehren. Der neue Benutzer sollte nun in der Liste **Benutzer** auf der Seite **Benutzerverwaltung** enthalten sein.
Bearbeiten eines Benutzers	Wählen Sie in der Liste **Benutzer** den Benutzer aus, den Sie bearbeiten möchten, und klicken Sie dann auf **Aktionen** | **Bearbeiten**. Die Seite **Benutzer bearbeiten** wird angezeigt. 1 Nehmen Sie die gewünschten Änderungen am Konto vor. 2 Klicken Sie auf **Speichern**. Die geänderten Benutzerdaten sollten nun in der Liste **Benutzer** auf der Seite **Benutzerverwaltung** enthalten sein.
Löschen eines Benutzers	Wählen Sie in der Liste **Benutzer** den Benutzer aus, den Sie löschen möchten, und klicken Sie dann auf **Aktionen** | **Löschen**. Ein Bestätigungsdialogfeld wird angezeigt. Klicken Sie auf **OK**. Der Benutzer sollte nun nicht mehr in der Liste **Benutzer** auf der Seite **Benutzerverwaltung** enthalten sein.

Erstellen einer benutzerdefinierten Anmeldenachricht

Sie können eine benutzerdefinierte Anmeldenachricht erstellen und anzeigen, die auf der Seite **Anmelden** erscheinen soll.

Die Nachricht kann als einfacher Text oder im HTML-Format geschrieben sein. Wenn Sie eine Nachricht im HTML-Format erstellen, sind Sie für alle Formatierungen und das Escaping verantwortlich.

Vorgehensweise

Definitionen zu Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

1. Klicken Sie auf **Menü** | **Konfiguration** | **Server-Einstellungen**, wählen Sie in der Liste **Einstellungskategorien** den Eintrag **Anmeldenachricht** aus, und klicken Sie dann auf **Bearbeiten**.

2. Wählen Sie **Benutzerdefinierte Anmeldenachricht anzeigen** aus, geben Sie die gewünschte Nachricht ein, und klicken Sie anschließend auf **Speichern**.

Konfigurieren einer Active Directory-Benutzeranmeldung

Durch die Konfiguration einer Active Directory-Benutzeranmeldung können Sie den Arbeitsaufwand senken, der mit der Verwaltung der Benutzerkonten sowie des Benutzerzugriffs verbunden ist.

Inhalt

Verwalten von ePolicy Orchestrator-Benutzern mit Active Directory

Sie können vorhandene Windows-authentifizierte Benutzeranmeldeinformationen verwenden, um automatisch ePolicy Orchestrator-Benutzer zu erstellen und diesen Berechtigungen zuzuweisen.

Dies wird erreicht, indem ePolicy Orchestrator-Berechtigungssätze zu Active Directory-Gruppen in Ihrer Umgebung zugeordnet werden. Bei einer großen Anzahl von ePolicy Orchestrator-Benutzern in einem Unternehmen kann mit dieser Funktion der Verwaltungsaufwand verringert werden. Gehen Sie folgendermaßen vor, um die Konfiguration vorzunehmen:

- Konfigurieren Sie die Benutzerauthentifizierung.
- Registrieren Sie die LDAP-Server.
- Weisen Sie der Active Directory-Gruppe Berechtigungssätze zu.

Benutzerauthentifizierung

ePolicy Orchestrator-Benutzer können mittels ePolicy Orchestrator-Kennwortauthentifizierung oder Windows-Authentifizierung authentifiziert werden. Bei Verwendung der Windows-Authentifizierung können Sie angeben, nach welchen Merkmalen Benutzer authentifiziert werden:

- Anhand der Domäne, zu der Ihr McAfee ePO-Server gehört (Standardeinstellung)
- Anhand einer Liste mit einem oder mehreren Domänen-Controllern
- Anhand einer Liste mit einem oder mehreren Domänennamen im DNS-Format
- Mithilfe eines WINS-Servers zum Auffinden des entsprechenden Domänen-Controllers

Wenn Sie Domänen-Controller, DNS-Domänennamen oder einen WINS-Server verwenden, müssen Sie die Server-Einstellung **Windows-Authentifizierung** konfigurieren.

Registrierte LDAP-Server

Sie müssen LDAP-Server bei Ihrem McAfee ePO-Server registrieren, um dynamisch zugewiesene Berechtigungssätze für Windows-Benutzer zuzulassen. Dynamisch zugewiesene Berechtigungssätze sind Berechtigungssätze, die Benutzern anhand deren Mitgliedschaft in Active Directory-Gruppen zugeordnet werden.



Benutzer, denen über unidirektionale externe Vertrauensstellungen vertraut wird, werden nicht unterstützt.

Das Benutzerkonto, mit dem der LDAP-Server bei ePolicy Orchestrator registriert ist, muss über eine bidirektionale transitive Vertrauensstellung als vertrauenswürdig gelten, oder es muss in der Domäne physisch vorhanden sein, zu der der LDAP-Server gehört.

Windows-Autorisierung

Die Server-Einstellung für die Windows-Autorisierung gibt an, welchen Active Directory-Server ePolicy Orchestrator verwendet, um Benutzer- und Gruppeninformationen für eine bestimmte Domäne zu sammeln. Sie können mehrere Domänen-Controller und Active Directory-Server angeben. Mit dieser Server-Einstellung können Sie Benutzern, die beim Anmelden Windows-Anmeldeinformationen angeben, Berechtigungssätze dynamisch zuweisen.



ePolicy Orchestrator kann Windows-authentifizierten Benutzern selbst bei deaktivierter Active Directory-Benutzeranmeldung Berechtigungssätze dynamisch zuweisen.

Zuweisen von Berechtigungen

Sie müssen mindestens einen Berechtigungssatz zu einer Active Directory-Gruppe zuweisen, bei der es sich nicht um die primäre Gruppe eines Benutzers handelt. Das dynamische Zuweisen von Berechtigungssätzen zur primären Gruppe eines Benutzers wird nicht unterstützt und führt dazu, dass nur die Berechtigungen gelten, die diesem Benutzer manuell zugewiesen wurden. In der Standardeinstellung ist "Domänen-Benutzer" die primäre Gruppe.

Active Directory-Benutzeranmeldung

Wenn Sie die oben aufgeführten Punkte konfiguriert haben, können Sie die Server-Einstellung zur automatischen Benutzererstellung aktivieren. Mithilfe automatischer Benutzererstellung können Benutzerdatensätze unter den folgenden Bedingungen automatisch erstellt werden:

- Benutzer geben gültige Anmeldeinformationen im Format <Domäne\Name> an. So würde zum Beispiel ein Benutzer mit dem Windows-Anmeldenamen "mmustermann1", der Mitglied in der Windows-Domäne "deu" ist, die folgenden Anmeldeinformationen angeben: "deu\mmustermann1" und das entsprechende Kennwort.
- Ein Active Directory-Server, der Informationen zu diesem Benutzer enthält, wurde bei ePolicy Orchestrator registriert.
- Der Benutzer ist Mitglied in mindestens einer Gruppe vom Typ "Lokal (in Domäne)" oder "Global (in Domäne)", die einem ePolicy Orchestrator-Berechtigungssatz zugeordnet ist.

Strategien für die Windows-Authentifizierung und -Autorisierung

Es gibt verschiedene Ansätze, nach denen Sie beim Planen der Registrierung Ihrer LDAP-Server vorgehen können. Wenn Sie sich im Vorfeld ausreichend Zeit für die Planung einer Strategie für die

Server-Registrierung nehmen, werden Sie gleich beim ersten Mal alles richtig machen und haben auch weniger Probleme bei der Benutzerauthentifizierung.

Im Idealfall müssen Sie diesen Vorgang nur einmal durchführen und Änderungen nur dann vornehmen, wenn sich Ihre Netzwerktopologie insgesamt ändert. Sobald die Server registriert sind und die Windows-Authentifizierung konfiguriert ist, sollten Sie diese Einstellungen nicht mehr allzu oft ändern müssen.

Vergleich von Authentifizierung und Autorisierung

Bei der Authentifizierung wird die Identität eines Benutzers verifiziert. Dabei werden die vom Benutzer angegebenen Anmeldeinformationen mit Informationen verglichen, denen das System als authentisch vertraut. Das können ein ePolicy Orchestrator-Server-Konto, Active Directory-Anmeldeinformationen oder ein Zertifikat sein. Wenn Sie die Windows-Authentifizierung verwenden möchten, müssen Sie untersuchen, auf welche Weise die Domänen (oder Server) organisiert sind, in denen sich Ihre Benutzerkonten befinden.

Die Autorisierung erfolgt, nachdem die Anmeldeinformationen eines Benutzers überprüft wurden. Hierbei werden Berechtigungssätze angewendet, die bestimmen, was der Benutzer innerhalb des Systems durchführen darf. Bei Verwendung der Windows-Authentifizierung können Sie festlegen, welche Aktionen Benutzern aus unterschiedlichen Domänen erlaubt sein sollen. Dies erfolgt über Berechtigungssätze, die Gruppen in diesen Domänen zugewiesen werden.

Netzwerktopologie für Benutzerkonten

Welche Schritte zur vollständigen Konfiguration der Windows-Authentifizierung und -Autorisierung erforderlich sind, richtet sich nach der Netzwerktopologie und der Verteilung der Benutzerkonten im Netzwerk.

- Wenn sich die Anmeldeinformationen für Ihre zukünftigen Benutzer alle in einer kleinen Auswahl von Domänen (oder Server) innerhalb einer einzigen Domänenstruktur befinden, müssen Sie nur den Stamm dieser Struktur registrieren – mehr nicht.
- Wenn Ihre Benutzerkonten breiter verteilt sind, müssen Sie eine größere Anzahl von Servern oder Domänen registrieren. Ermitteln Sie, wie viele Domänen-Unterstrukturen (oder Server-Unterstrukturen) Sie mindestens benötigen, und registrieren Sie die Stämme dieser Strukturen. Versuchen Sie, diese in der Reihenfolge zu registrieren, in der sie am häufigsten verwendet werden. Da die Liste der Domänen (oder Server) beim Authentifizierungsvorgang in der aufgeführten Reihenfolge durchlaufen wird, wirkt es sich positiv auf die durchschnittliche Authentifizierungsleistung aus, wenn sich die am häufigsten verwendeten Domänen oder Server oben in der Liste befinden.

Berechtigungsstruktur

Damit ein Benutzer sich mittels Windows-Authentifizierung bei einem ePolicy Orchestrator-Server anmelden kann, muss mit der in seiner Domäne befindlichen Active Directory-Gruppe, zu der sein Konto gehört, ein Berechtigungssatz verbunden sein. Bei der Frage, wie Berechtigungssätze zugewiesen sein sollen, müssen Sie folgende Punkte beachten:

- Berechtigungssätze können mehreren Active Directory-Gruppen zugewiesen werden.
- Berechtigungssätze können dynamisch nur einer gesamten Active Directory-Gruppe zugewiesen werden. Sie können nicht nur einigen Benutzern aus einer Gruppe zugewiesen werden.

Wenn Sie einem einzelnen Benutzer spezielle Berechtigungen zuweisen möchten, können Sie dies durchführen, indem Sie eine Active Directory-Gruppe erstellen, in der sich nur dieser jeweilige Benutzer befindet.

Konfigurieren von Windows-Authentifizierung und -Autorisierung

Gehen Sie wie in diesen Aufgaben beschrieben vor, um die Active Directory-Benutzeranmeldung einzurichten.

Aufgaben

- *Aktivieren der Windows-Authentifizierung im McAfee ePO-Server* auf Seite 40
  Bevor die erweiterte Windows-Authentifizierung verwendet werden kann, muss der Server entsprechend vorbereitet werden.
- *Konfigurieren der Windows-Authentifizierung* auf Seite 40
  Es gibt mehrere Möglichkeiten, wie vorhandene Anmeldeinformationen für Windows-Konten in ePolicy Orchestrator verwendet werden können.
- *Konfigurieren der Windows-Autorisierung* auf Seite 41
  Damit Benutzer sich erfolgreich mittels Windows-Authentifizierung beim ePolicy Orchestrator-Server anmelden können, benötigen sie einen Berechtigungssatz, der einer ihrer Active Directory-Gruppen zugewiesen ist.

Aktivieren der Windows-Authentifizierung im McAfee ePO-Server

Bevor die erweiterte Windows-Authentifizierung verwendet werden kann, muss der Server entsprechend vorbereitet werden.

Zum Aktivieren der Seite **Windows-Authentifizierung** in den **Server-Einstellungen** müssen Sie zuerst den ePolicy Orchestrator-Dienst beenden. Dieser Schritt muss direkt auf dem McAfee ePO-Server ausgeführt werden.

Vorgehensweise

Definitionen zu Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

1. Klicken Sie in der Server-Konsole auf **Start | Einstellungen | Systemsteuerung | Verwaltung**.
2. Wählen Sie **Dienste** aus.
3. Klicken Sie im Fenster **Dienste** mit der rechten Maustaste auf **McAfee ePolicy Orchestrator-Anwendungs-Server**, und wählen Sie **Beenden** aus.
4. Benennen Sie die Datei `WINAUTH.DLL` in `WINAUTH.BAK` um.

   In einer Standardinstallation befindet sich diese Datei in `C:\Programme\McAfee\ePolicy Orchestrator\Server\bin`.
5. Starten Sie den Server neu.

Wenn Sie die Seite **Server-Einstellungen** das nächste Mal öffnen, wird die Option **Windows-Authentifizierung** angezeigt.

Konfigurieren der Windows-Authentifizierung

Es gibt mehrere Möglichkeiten, wie vorhandene Anmeldeinformationen für Windows-Konten in ePolicy Orchestrator verwendet werden können.

> **Bevor Sie beginnen**
>
> Sie müssen Ihren Server zunächst für die Windows-Authentifizierung vorbereitet haben.

Wie Sie diese Einstellungen konfigurieren, hängt von verschiedenen Aspekten ab:

- Möchten Sie mehrere Domänen-Controller verwenden?
- Sind die Benutzer über mehrere Domänen verteilt?
- Möchten Sie mithilfe eines WINS-Servers suchen, anhand welcher Domäne Benutzer authentifiziert werden sollen?

Ohne besondere Konfiguration können sich Benutzer mit Windows-Anmeldeinformationen für die Domäne authentifizieren, zu der der McAfee ePO-Server gehört, oder mit Anmeldeinformationen jeder anderen Domäne, die in einer wechselseitigen Vertrauensstellung zur Domäne des McAfee ePO-Servers steht. Wenn Benutzer aus Domänen vorhanden sind, die diese Kriterien nicht erfüllen, müssen Sie die Windows-Authentifizierung konfigurieren.

Vorgehensweise

Definitionen zu Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

1. Klicken Sie auf **Menü** | **Konfiguration** | **Server-Einstellungen**, und klicken Sie dann in der Liste **Einstellungskategorien** auf **Windows-Authentifizierung**.
2. Klicken Sie auf **Bearbeiten**.
3. Geben Sie an, ob Sie eine oder mehrere Domänen, einen oder mehrere Domänen-Controller oder einen WINS-Server verwenden möchten.

   Domänen müssen im DNS-Format angegeben werden (z. B. `interneDomäne.com`). Domänen-Controller und WINS-Server müssen vollqualifizierte Domänennamen haben (z. B. `dc.interneDomäne.com`).

   Sie können mehrere Domänen oder Domänen-Controller, aber nur einen WINS-Server angeben. Klicken Sie auf **+**, um weitere Domänen oder Domänen-Controller zur Liste hinzuzufügen.

4. Wenn Sie alle gewünschten Server hinzugefügt haben, klicken Sie auf **Speichern**.

Wenn Sie Domänen oder Domänen-Controller angeben, geht der McAfee ePO-Server beim Authentifizieren von Benutzern die Server in der aufgeführten Reihenfolge durch. Zuerst wird die Authentifizierung beim ersten in der Liste eingetragenen Server versucht, und dann wird die Liste abwärts abgearbeitet, bis ein Benutzer erfolgreich authentifiziert ist.

Konfigurieren der Windows-Autorisierung

Damit Benutzer sich erfolgreich mittels Windows-Authentifizierung beim ePolicy Orchestrator-Server anmelden können, benötigen sie einen Berechtigungssatz, der einer ihrer Active Directory-Gruppen zugewiesen ist.

Vorgehensweise

Definitionen zu Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

1. Klicken Sie auf **Menü** | **Benutzerverwaltung** | **Berechtigungssätze**.
2. Wählen Sie entweder in der Liste **Berechtigungssätze** einen vorhandenen Berechtigungssatz aus, und klicken Sie dann im Abschnitt **Name und Benutzer** auf **Bearbeiten**, oder klicken Sie auf **Aktionen** | **Neu**.
3. Wählen Sie einzelne Benutzer aus, für die der Berechtigungssatz gilt.
4. Wählen Sie in der Liste einen **Server-Namen** aus, und klicken Sie auf **Hinzufügen**.

5 Wechseln Sie im LDAP-Browser zu den Gruppen, für die dieser Berechtigungssatz gilt, und wählen Sie sie aus.

   Wenn Sie im Bereich **Durchsuchen** ein Element auswählen, werden im Bereich **Gruppen** die Mitglieder dieses Elements angezeigt. Sie können eine beliebige Anzahl dieser Gruppen auswählen, die den Berechtigungssatz dynamisch erhalten sollen. Es können immer nur Mitglieder aus einem Element gleichzeitig hinzugefügt werden. Für Mitglieder aus mehreren Elementen müssen Sie die Schritte 4 und 5 so lange wiederholen, bis alle gewünschten Mitglieder hinzugefügt sind.

6 Klicken Sie auf **Speichern**.

Der Berechtigungssatz wird jetzt auf alle Benutzer aus den angegebenen Gruppen angewendet, die sich mittels Windows-Authentifizierung beim Server anmelden.

Client-Zertifikatauthentifizierung

Clients können ein digitales Zertifikat als Anmeldeinformationen für die Authentifizierung verwenden, wenn sie sich bei einem McAfee ePO-Server anmelden.

Inhalt

Verwenden der Client-Zertifikatauthentifizierung

Die Client-Zertifikatauthentifizierung ist die sicherste der zur Verfügung stehenden Methoden. Sie ist jedoch nicht in jeder Umgebung auch die beste Wahl.

Die Client-Zertifikatauthentifizierung ist eine Erweiterung der Authentifizierung mit öffentlichem Schlüssel. Als Grundlage dienen öffentliche Schlüssel, aber anders als bei der Authentifizierung mit öffentlichem Schlüssel muss nur einem vertrauenswürdigen Drittanbieter vertraut werden, der als *Zertifizierungsstelle* bekannt ist. Zertifikate sind digitale Dokumente, die eine Kombination von Identitätsinformationen und öffentlichen Schlüsseln enthalten und von der Zertifizierungsstelle, die die Richtigkeit der Informationen überprüft, digital signiert werden.

Vorteile zertifikatbasierter Authentifizierung

Die zertifikatbasierte Authentifizierung weist gegenüber der Authentifizierung mittels Kennwort mehrere Vorteile auf:

- Zertifikate haben eine vorab festgelegte Gültigkeitsdauer. Dadurch wird eine erzwungene, periodische Überprüfung der Berechtigungen eines Benutzers bei Ablauf des Zertifikats ermöglicht.
- Wenn der Zugriff eines Benutzers gesperrt oder beendet werden muss, kann das Zertifikat zu einer *Zertifikatsperrliste* hinzugefügt werden, die bei jedem Anmeldeversuch geprüft wird, um unbefugten Zugriff zu vermeiden.
- Da nur einer geringen Anzahl von Zertifizierungsstellen – meist nur einer – vertraut werden muss, ist die zertifikatbasierte Authentifizierung in großen Institutionen leichter zu verwalten und besser skalierbar als andere Formen der Authentifizierung.

Nachteile zertifikatbasierter Authentifizierung

Nicht jede Umgebung ist für eine zertifikatbasierte Authentifizierung geeignet. Zu den Nachteilen dieser Methode gehören:

- Es ist eine Infrastruktur mit öffentlichem Schlüssel erforderlich. Dadurch können zusätzliche Kosten entstehen, die in einigen Fällen das Mehr an Sicherheit nicht wert sind.
- Im Vergleich zur Authentifizierung mittels Kennwort bringt diese Methode einen zusätzlichen Arbeitsaufwand beim Verwalten von Zertifikaten mit sich.

Konfigurieren von ePolicy Orchestrator für die Client-Zertifikatauthentifizierung

Damit sich Benutzer mithilfe der zertifikatbasierten Authentifizierung anmelden können, muss ePolicy Orchestrator entsprechend konfiguriert werden.

Bevor Sie beginnen

Sie müssen ein signiertes Zertifikat im Format P7B, PKCS12, DER oder PEM besitzen.

Vorgehensweise

1. Klicken Sie auf **Menü** | **Konfiguration** | **Server-Einstellungen**.
2. Wählen Sie **Zertifikatbasierte Authentifizierung** aus, und klicken Sie auf **Bearbeiten**.
3. Wählen Sie **Zertifikatbasierte Authentifizierung aktivieren** aus.
4. Klicken Sie neben **Client-Zertifikat der Zertifizierungsstelle** auf die Schaltfläche **Durchsuchen**.
5. Wechseln Sie zu der Zertifikatdatei, wählen Sie sie aus, und klicken Sie auf **OK**.
6. Wenn Sie über eine **Datei mit Zertifikatsperrliste** (CRL-Datei) verfügen, klicken Sie neben diesem Bearbeitungsfeld auf die Schaltfläche **Durchsuchen**, wechseln Sie zu der CRL-Datei, und klicken Sie auf **OK**.
7. Klicken Sie auf **Speichern**, um alle Änderungen zu speichern.
8. Starten Sie ePolicy Orchestrator neu, um die zertifikatbasierte Authentifizierung zu aktivieren.

Ändern der zertifikatbasierten Authentifizierung von ePolicy Orchestrator-Server

Server benötigen Zertifikate für SSL-Verbindungen, die höhere Sicherheit als Standard-HTTP-Sitzungen bieten.

Bevor Sie beginnen

Um ein signiertes Zertifikat hochladen zu können, müssen Sie bereits ein Server-Zertifikat von einer Zertifizierungsstelle erhalten haben.

Sie können auch selbstsignierte Zertifikate anstelle von extern signierten Zertifikaten verwenden, dies birgt jedoch ein etwas höheres Risiko. Mit der nachfolgend beschriebenen Vorgehensweise kann eine zertifikatbasierte Authentifizierung erstmalig konfiguriert oder eine vorhandene Konfiguration mit einem aktualisierten Zertifikat geändert werden.

Vorgehensweise

Definitionen zu Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

1. Klicken Sie auf **Menü** | **Konfiguration** | **Server-Einstellungen**.
2. Wählen Sie **Zertifikatbasierte Authentifizierung** aus, und klicken Sie auf **Bearbeiten**.
3. Wählen Sie **Zertifikatbasierte Authentifizierung aktivieren** aus.
4. Klicken Sie neben **Client-Zertifikat der Zertifizierungsstelle** auf die Schaltfläche **Durchsuchen**. Wechseln Sie zu der Zertifikatdatei, wählen Sie sie aus, und klicken Sie auf **OK**.

   Sobald eine Datei übernommen wurde, ändert sich die Eingabeaufforderung zu **Aktuelles Zertifizierungsstellen-Zertifikat ersetzen**.

5. Wenn Sie eine PKCS12-Zertifikatdatei angegeben haben, geben Sie ein Kennwort ein.
6. Wenn Sie eine Datei mit Zertifikatsperrliste (CRL) bereitstellen möchten, klicken Sie neben **Datei mit Zertifikatsperrliste (PEM)** auf **Durchsuchen**. Wechseln Sie zur Zertifikatsperrlisten-Datei, wählen Sie sie aus, und klicken Sie auf **OK**.

   Die Zertifikatsperrlisten-Datei muss im PEM-Format vorliegen.

7. Falls erforderlich, wählen Sie erweiterte Einstellungen aus.
8. Klicken Sie auf **Speichern**, um alle Änderungen zu speichern.
9. Starten Sie den Server neu, um die Änderungen an den Einstellungen von **Zertifikatbasierte Authentifizierung** zu aktivieren.

Deaktivieren der Client-Zertifikatauthentifizierung von ePolicy Orchestrator-Server

Server-Zertifikate können und sollten deaktiviert werden, wenn sie nicht mehr verwendet werden.

Bevor Sie beginnen

Bevor Sie Server-Zertifikate deaktivieren können, muss der Server bereits für die Client-Zertifikatauthentifizierung konfiguriert sein.

Nachdem ein Server-Zertifikat geladen wurde, kann es nur noch deaktiviert, aber nicht mehr entfernt werden.

Vorgehensweise

Definitionen zu Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

1. Öffnen Sie die Seite **Server-Einstellungen**, indem Sie **Menü** | **Konfiguration** | **Server-Einstellungen** auswählen.
2. Wählen Sie **Zertifikatbasierte Authentifizierung** aus, und klicken Sie auf **Bearbeiten**.
3. Deaktivieren Sie **Zertifikatbasierte Authentifizierung aktivieren**, und klicken Sie dann auf **Speichern**.

Die Server-Einstellungen wurden geändert. Sie müssen den Server jedoch neu starten, um den Vorgang abzuschließen.

Konfigurieren von Benutzern für zertifikatbasierte Authentifizierung

Damit Benutzer sich mit ihren digitalen Zertifikaten anmelden können, muss die zertifikatbasierte Authentifizierung konfiguriert sein.

Die für die zertifikatbasierte Authentifizierung verwendeten Zertifikate befinden sich meist auf einer Smartcard oder einem ähnlichen Gerät. Die Zertifikatdatei kann mithilfe einer Software aus dem Lieferumfang der Smartcard-Hardware extrahiert werden. Diese extrahierte Zertifikatdatei ist normalerweise die Datei, die in dem hier beschriebenen Verfahren hochgeladen wird.

Vorgehensweise

Definitionen zu Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

1. Klicken Sie auf **Menü** | **Benutzerverwaltung** | **Benutzer**.
2. Wählen Sie einen Benutzer aus, und klicken Sie auf **Aktionen** | **Bearbeiten**.
3. Wählen Sie **Authentifizierung oder Anmeldeinformationen ändern** aus, und wählen Sie dann **Zertifikatbasierte Authentifizierung** aus.
4. Geben Sie die Anmeldeinformationen nach einer der hier beschriebenen Methoden an.
   - Kopieren Sie das Feld für den eindeutigen Namen (DN-Feld) aus der Zertifikatdatei, und fügen Sie es in das Bearbeitungsfeld **Betrefffeld für eindeutigen Namen des persönlichen Zertifikats** ein.
   - Laden Sie die Zertifikatdatei hoch, die mit dem Zertifizierungsstellen-Zertifikat signiert wurde, das Sie im Abschnitt *Konfigurieren von ePolicy Orchestrator für die zertifikatbasierte Authentifizierung* hochgeladen haben. Klicken Sie auf **Durchsuchen**, wechseln Sie zu der Zertifikatdatei auf Ihrem Computer, wählen Sie sie aus, und klicken Sie auf **OK**.

   Benutzerzertifikate können PEM- oder DER-codiert sein. Solange das Format X.509- oder PKCS12-konform ist, spielt es jedoch keine Rolle, in welchem Format das Zertifikat vorliegt.
5. Klicken Sie auf **Speichern**, um die an der Konfiguration des Benutzers vorgenommenen Änderungen zu speichern.

Die angegebenen Zertifikatinformationen werden überprüft. Falls sie ungültig sind, wird eine Warnung ausgegeben. Wenn ein Benutzer versucht, sich bei ePolicy Orchestrator von einem Browser aus anzumelden, auf dem sein Zertifikat installiert ist, wird von nun an das Anmeldeformular ausgegraut angezeigt und der Benutzer sofort authentifiziert.

Aktualisieren der CRL-Datei

Sie können die auf dem McAfee ePO-Server installierte CRL-Datei (Zertifikatsperrliste) aktualisieren, um den Zugriff bestimmter Benutzer auf ePolicy Orchestrator zu unterbinden.

Bevor Sie beginnen

Es muss bereits eine CRL-Datei im ZIP- oder PEM-Format vorliegen.

Die CRL-Datei besteht aus einer Liste gesperrter ePolicy Orchestrator-Benutzer mit dem Status ihrer digitalen Zertifikate. Die Liste enthält die gesperrten Zertifikate, die Gründe für die Sperrung, den Zeitpunkt der Zertifikatsaustellung und die ausstellende Körperschaft. Wenn ein Benutzer versucht, auf den McAfee ePO-Server zuzugreifen, wird in der CRL-Datei geprüft, ob dem Benutzer der Zugriff gewährt werden darf oder nicht.

Vorgehensweise

1. Klicken Sie auf **Menü** | **Konfiguration** | **Server-Einstellungen**.
2. Wählen Sie **Zertifikatbasierte Authentifizierung** aus, und klicken Sie auf **Bearbeiten**.
3. Klicken Sie zum Aktualisieren der **Datei mit Zertifikatsperrliste** (CRL-Datei) auf die Schaltfläche **Durchsuchen** neben diesem Bearbeitungsfeld, wechseln Sie zur CRL-Datei, und klicken Sie dann auf **OK**.
4. Klicken Sie auf **Speichern**, um alle Änderungen zu speichern.
5. Starten Sie ePolicy Orchestrator neu, um die zertifikatbasierte Authentifizierung zu aktivieren.

   Sie können die CRL-Datei auch mithilfe der cURL-Befehlszeile aktualisieren. Geben Sie dazu in der cURL-Befehlszeile Folgendes ein:

   Damit cURL-Befehle per Befehlszeile ausgeführt werden können, muss cURL installiert sein, und Sie müssen Remote-Zugriff auf den McAfee ePO-Server haben. Ausführliche Informationen zum Download von cURL und weitere Beispiele finden Sie im *Skripthandbuch zu ePolicy Orchestrator 5.0.0*.

   ```
   curl -k --cert <Admin-Zertifikat>.pem --key <Admin-Schlüssel>.pem https://
   <localhost>:<Port>/remote/console.cert.updatecrl.do -F crlFile=@<CRLs>.zip
   ```

   Die einzelnen Parameter bedeuten Folgendes:

   - `<Admin-Zertifikat>` – Der Name der PEM-Datei mit dem Administrator-Client-Zertifikat
   - `<Admin-Schlüssel>` – Der Name der PEM-Datei mit dem privaten Administrator-Client-Schlüssel
   - `<localhost>:<Port>` – Name und Nummer des Kommunikationsports des McAfee ePO-Servers
   - `<CRLs>` – Der Name der CRL-PEM- oder -ZIP-Datei

Nun wird bei jedem Zugriff eines Benutzers auf den McAfee ePO-Server in der neuen CRL-Datei geprüft, ob die zertifikatbasierte Authentifizierung für diesen Benutzer widerrufen wurde.

Probleme bei der Client-Zertifikatauthentifizierung

Die meisten Probleme bei der zertifikatbasierten Authentifizierung werden von einer kleinen Anzahl von Problemen verursacht.

Wenn sich ein Benutzer mit seinem Zertifikat nicht bei ePolicy Orchestrator anmelden kann, sollten Sie eine der folgenden Möglichkeiten ausprobieren, um das Problem zu beheben:

- Stellen Sie sicher, dass der Benutzer nicht deaktiviert wurde.
- Überprüfen Sie, ob das Zertifikat abgelaufen ist oder zurückgenommen wurde.

- Überprüfen Sie, ob das Zertifikat von der richtigen Zertifizierungsstelle signiert wurde.
- Überprüfen Sie, ob das Feld für den eindeutigen Namen auf der Benutzerkonfigurationsseite korrekt ist.
- Vergewissern Sie sich, dass der Browser das richtige Zertifikat angibt.
- Überprüfen Sie das Audit-Protokoll auf Authentifizierungsmeldungen.

SSL-Zertifikate

Die von McAfee ePO unterstützten Browser zeigen eine Warnung bezüglich eines SSL-Zertifikats des Servers an, wenn nicht überprüft werden kann, dass ein Zertifikat gültig ist oder von einer vertrauenswürdigen Quelle signiert wurde. Der McAfee ePO-Server verwendet für die SSL-Kommunikation mit dem Web-Browser standardmäßig ein selbstsigniertes Zertifikat, das vom Browser in der Standardeinstellung nicht als vertrauenswürdig angesehen wird. Daher wird jedes Mal, wenn Sie zur McAfee ePO-Konsole wechseln, eine Warnmeldung angezeigt.

Wenn diese Warnung nicht mehr angezeigt werden soll, müssen Sie einen der folgenden Schritte durchführen:

- Fügen Sie das McAfee ePO-Server-Zertifikat zur Sammlung der vom Browser verwendeten vertrauenswürdigen Zertifikate hinzu.



Diesen Schritt müssen Sie für jeden einzelnen Browser vornehmen, der mit McAfee ePO interagiert. Wenn sich das Server-Zertifikat ändert, müssen Sie das McAfee ePO-Server-Zertifikat erneut hinzufügen, da das vom Server gesendete Server-Zertifikat nicht mehr mit dem Zertifikat übereinstimmt, zu dessen Verwendung der Browser konfiguriert wurde.

- Ersetzen Sie das standardmäßige McAfee ePO-Server-Zertifikat durch ein gültiges Zertifikat, das von einer Zertifizierungsstelle signiert wurde, der der Browser vertraut. Das ist der beste Weg. Da das Zertifikat von einer vertrauenswürdigen Zertifizierungsstelle signiert wurde, müssen Sie es nicht zu sämtlichen Web-Browsern in Ihrem Unternehmen hinzufügen.



Wenn sich der Server-Hostname ändert, können Sie das Server-Zertifikat durch ein anderes Zertifikat ersetzen, das ebenfalls von einer vertrauenswürdigen Zertifizierungsstelle signiert wurde.

Um das McAfee ePO-Server-Zertifikat ersetzen zu können, müssen Sie zuerst ein neues Zertifikat erhalten – vorzugsweise ein Zertifikat, das von einer vertrauenswürdigen Zertifizierungsstelle signiert wurde. Außerdem benötigen Sie den privaten Schlüssel des Zertifikats und dessen Kennwort (sofern vorhanden). Dann können Sie mit all diesen Dateien das Zertifikat des Servers ersetzen. Weitere Informationen zum Ersetzen von Server-Zertifikaten finden Sie unter *Beschreibung und Funktionsweise von Sicherheitsschlüsseln*.

Der McAfee ePO-Browser erwartet, dass die verknüpften Dateien das folgende Format verwenden:

- Server-Zertifikat – P7B oder PEM
- Privater Schlüssel – PEM

Wenn das Server-Zertifikat oder der private Schlüssel in einem anderen Format vorliegen, müssen sie in eines der unterstützten Formate konvertiert werden, bevor sie zum Ersetzen des Server-Zertifikats verwendet werden können.

Ersetzen des Server-Zertifikats

In den **Server-Einstellungen** können Sie das Server-Zertifikat und den privaten Schlüssel angeben, die von ePolicy Orchestrator verwendet werden.

Vorgehensweise

Definitionen zu Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

1. Klicken Sie auf **Menü** | **Konfiguration** | **Server-Einstellungen**, und klicken Sie dann in der Liste **Einstellungskategorien** auf **Server-Zertifikat**.
2. Klicken Sie auf **Bearbeiten**. Die Seite **Server-Zertifikat: Bearbeiten** wird angezeigt.
3. Wechseln Sie zu der Datei mit dem Server-Zertifikat, und klicken Sie auf **Öffnen**.
4. Wechseln Sie zu der Datei mit dem privaten Schlüssel, und klicken Sie auf **Öffnen**.
5. Geben Sie bei Bedarf das Kennwort für den privaten Schlüssel ein.
6. Klicken Sie auf **Speichern**.



Nachdem Sie das neue Zertifikat und den neuen privaten Schlüssel übernommen haben, müssen Sie ePolicy Orchestrator neu starten, damit die Änderungen wirksam werden.

Installieren eines vertrauenswürdigen Sicherheitszertifikats für den McAfee ePO-Browser

Sie können ein vertrauenswürdiges Sicherheitszertifikat für Ihren McAfee ePO-Browser installieren, damit nicht bei jeder Anmeldung eine Sicherheitswarnung angezeigt wird.

Aufgaben

- *Installieren des Sicherheitszertifikats bei Verwendung von Internet Explorer* auf Seite 48
  Bei Verwendung unterstützter Versionen von Internet Explorer können Sie das Sicherheitszertifikat installieren, damit nicht bei jeder Anmeldung das Dialogfeld mit dem Warnhinweis angezeigt wird.
- *Installieren des Sicherheitszertifikats bei Verwendung von Firefox 3.5 (oder höher)* auf Seite 49
  Bei Verwendung von Firefox 3.5 (oder höher) können Sie das Sicherheitszertifikat installieren, damit nicht bei jeder Anmeldung das Dialogfeld mit dem Warnhinweis angezeigt wird.

Installieren des Sicherheitszertifikats bei Verwendung von Internet Explorer

Bei Verwendung unterstützter Versionen von Internet Explorer können Sie das Sicherheitszertifikat installieren, damit nicht bei jeder Anmeldung das Dialogfeld mit dem Warnhinweis angezeigt wird.

Vorgehensweise

1. Starten Sie ePolicy Orchestrator in einem Browser. Klicken Sie auf **Zertifikatfehler**. Die Seite **Navigation wurde geblockt** wird geöffnet.
2. Klicken Sie auf **Laden dieser Website fortsetzen (nicht empfohlen)**, um die Anmeldeseite zu öffnen. Die Adressleiste ist rot, wodurch angezeigt wird, dass der Browser das Sicherheitszertifikat nicht verifizieren kann.
3. Klicken Sie rechts neben der Adressleiste auf **Zertifikatfehler**, um die Warnung **Zertifikat ist ungültig** anzuzeigen.
4. Klicken Sie unten in der Warnung auf **Zertifikate anzeigen**, um das Dialogfeld **Zertifikat** zu öffnen.



Klicken Sie auf der Registerkarte **Allgemein** nicht auf **Zertifikat installieren**. Andernfalls schlägt der Vorgang fehl.

5 Klicken Sie auf die Registerkarte **Zertifizierungspfad**, wählen Sie dann **Orion_CA_<Server-Name>** aus, und klicken Sie auf **Zertifikat anzeigen**. Auf der Registerkarte **Allgemein** wird ein weiteres Dialogfeld **Zertifikat** geöffnet, in dem die **Zertifikatsinformationen** angezeigt werden.

6 Klicken Sie auf **Zertifikat installieren**, um den **Zertifikatsimport-Assistenten** zu öffnen.

7 Klicken Sie auf **Weiter**, um anzugeben, wo sich das Zertifikat befindet.

8 Wählen Sie **Alle Zertifikate in folgendem Speicher speichern** aus, und klicken Sie dann auf **Durchsuchen**, um einen Speicherort auszuwählen.

9 Wählen Sie in der Liste den Ordner **Vertrauenswürdige Stammzertifizierungsstellen** aus, klicken Sie auf **OK**, und klicken Sie dann auf **Weiter**.

10 Klicken Sie auf **Fertig stellen**. Klicken Sie in der daraufhin angezeigten **Sicherheitswarnung** auf **Ja**.

11 Schließen Sie den Browser.

12 Ändern Sie das Ziel der Desktop-Verknüpfung für ePolicy Orchestrator so, dass der NetBIOS-Name des ePolicy Orchestrator-Servers verwendet wird (statt "localhost").

13 Starten Sie ePolicy Orchestrator neu.

Von nun an werden Sie beim Anmelden bei ePolicy Orchestrator nicht mehr aufgefordert, das Zertifikat zu akzeptieren.

Installieren des Sicherheitszertifikats bei Verwendung von Firefox 3.5 (oder höher)

Bei Verwendung von Firefox 3.5 (oder höher) können Sie das Sicherheitszertifikat installieren, damit nicht bei jeder Anmeldung das Dialogfeld mit dem Warnhinweis angezeigt wird.

Vorgehensweise

1 Starten Sie ePolicy Orchestrator in einem Browser. Die Seite **Sichere Verbindung fehlgeschlagen** wird angezeigt.

2 Klicken Sie unten auf der Seite auf **Oder Sie können eine Ausnahme hinzufügen**. Nun wird auf der Seite die Schaltfläche **Ausnahme hinzufügen** angezeigt.

3 Klicken Sie auf **Ausnahme hinzufügen**. Das Dialogfeld **Sicherheits-Ausnahmeregel hinzufügen** wird angezeigt.

4 Klicken Sie auf **Zertifikat herunterladen**. Die Angaben zum **Zertifikat-Status** sind nun eingetragen, und die Schaltfläche **Sicherheits-Ausnahmeregel bestätigen** ist aktiviert.

5 Vergewissern Sie sich, dass **Diese Ausnahme dauerhaft speichern** aktiviert ist, und klicken Sie dann auf **Sicherheits-Ausnahmeregel bestätigen**.

Von nun an werden Sie beim Anmelden bei ePolicy Orchestrator nicht mehr aufgefordert, das Zertifikat zu akzeptieren.

Erstellen eines selbstsignierten Zertifikats mit OpenSSL

Manchmal können oder möchten Sie nicht warten, bis ein Zertifikat von einer Zertifizierungsstelle authentifiziert wurde. Bei ersten Tests oder bei Systemen, die in internen Netzwerken genutzt werden, kann ein selbstsigniertes Zertifikat ein ausreichendes Maß an Sicherheit und Funktionalität bieten.

Bevor Sie beginnen

Zum Erstellen eines selbstsignierten Zertifikats müssen Sie OpenSSL für Windows installieren. OpenSSL ist unter der folgenden URL-Adresse verfügbar:

http://www.slproweb.com/products/Win32OpenSSL.html

Verwenden Sie OpenSSL für Windows, wenn Sie ein Zertifikat für Ihren McAfee ePO-Server erstellen und selbst signieren möchten.



Es gibt viele Tools, mit denen selbstsignierte Zertifikate erstellt werden können. Hier wird die Vorgehensweise unter Verwendung von OpenSSL beschrieben.

Die im nachfolgenden Task verwendete Dateistruktur sieht wie folgt aus:



Diese Ordner werden nicht standardmäßig von OpenSSL nicht erstellt. Sie werden in diesen Beispielen verwendet und können erstellt werden, damit Sie Ihre Ausgabedateien leichter finden.

- **C:\ssl** – Der Installationsordner für OpenSSL.
- **C:\ssl\certs** – Hier werden die erstellten Zertifikate gespeichert.
- **C:\ssl\keys** – Hier werden die erstellten Schlüssel gespeichert.
- **C:\ssl\requests** – Hier werden die erstellten Zertifizierungsanforderungen gespeichert.

Vorgehensweise

1. Geben Sie den folgenden Befehl in einer Befehleszeile ein, um den anfänglichen Zertifikatschlüssel zu erstellen:

   ```
   C:\ssl\bin>openssl genrsa -des3 -out C:/ssl/keys/ca.key 1024
   ```

   Der folgende Bildschirm wird angezeigt.

   ```
   Loading 'screen' into random state - done
   Generating RSA private key, 1024 bit long modulus
   ........................++++++
   .++++++
   unable to write 'random state'
   e is 65537 (0x10001)
   Enter pass phrase for keys/ca.key:
   Verifying - Enter pass phrase for keys/ca.key:

   C:\ssl\bin>
   ```

2 Geben Sie bei der ersten Eingabeaufforderung eine Passphrase ein, und geben Sie diese dann zur Bestätigung ein zweites Mal ein.



Notieren Sie sich die von Ihnen eingegebene Passphrase gut. Sie werden sie im Folgenden noch benötigen.

Eine Datei mit dem Namen "ca.key" wird generiert und im Ordner **C:\ssl\keys** gespeichert.

Der Schlüssel sieht in etwa so aus:

```
-----BEGIN RSA PRIVATE KEY-----
Proc-Type: 4,ENCRYPTED
DEK-Info: DES-EDE3-CBC,CE327E8D510D1882

4Evg9bqeteKbo60Wy0cFh6o8gUhc0TDn/odppSeykvQBAasEhFfcF+nHLort8KkS
bS9WDAqczf6SdKMxoGbi9m57X/PZ+7dcTH7YyKNKskfoqED7/VZXktAEhA1Vw+wj
.
.
.
im2DEkLWQ3kI+6HdaQHo0Fe99ReHZJzvAU6F6LbUNULLpDe3wvnGwMI681fAF9C3
4+KDIt1RhfK3piLpCOM+8L1Dpd0g5FC723Z1Drr0uwghKdyD1GRKLw==
-----END RSA PRIVATE KEY-----
```

3 Geben Sie den folgenden Befehl in einer Befehlszeile ein, um den erstellten Zertifikatschlüssel selbst zu signieren:

```
openssl req -new -x509 -days 365 -key C:/ssl/keys/ca.key -out C:/ssl/certs/ca.cer
```

Der folgende Bildschirm wird angezeigt.

```
Enter pass phrase for ca.key:
Loading 'screen' into random state - done
You are about to be asked to enter information that will be
incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished
Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [AU]:US
State or Province Name (full name) [Some-State]:Oregon
Locality Name (eg, city) []:Beaverton
Organization Name (eg, company) [Internet Widgits Pty Ltd]:McAfee
Organizational Unit Name (eg, section) []:Enterprise
Common Name (eg, YOUR name) []:ePO_Server
Email Address []:tester@mcafee.com

C:\ssl\bin>
```

Geben Sie nach den folgenden Eingabeaufforderungen die erforderlichen Informationen ein:

- Country Name (2 letter code) [AU]:
- State or Province Name (full name) [Some-State]:
- Locality Name (eg, city) []:

- Organization Name (eg, company) [Internet Widgits Pty Ltd]:
- Organizational Unit Name (eg, section) []:
- Common Name (eg, YOUR name) []:



Geben Sie bei dieser Eingabeaufforderung den Namen Ihres Servers ein (z. B. den Namen Ihres McAfee ePO-Servers).

- Email Address []:

Eine Datei mit dem Namen "ca.cer" wird generiert und im Ordner **C:\ssl\certs** gespeichert.

Das selbstsignierte Zertifikat sieht in etwa wie folgt aus:

```
-----BEGIN CERTIFICATE-----
MIIDdTCCAt6gAwIBAgIJAJe1id+IhOGDMA0GCSqGSIb3DQEBBQUAMIGEMQswCQYD
VQQGEwJVUzEPMA0GA1UECBMGT1JFR090MRIwEAYDVQQHEw1CRUFWRVJUT04xDzAN
.
.
.
NF/Om6VMhuUy4Cyc5CIyTmGzVPDEo8dK20kdLR+tQhDsdqM5qpfd6w52ew20RKo/
dLGiMtraicXeR2GyWrKJjywow3xBtkvyQQj2xmMWUmDwYjCOYHO1KjVOX+fGwcdX
jWTfB10HV8507ASUOqte0we/BSTMuZWgMA==
-----END CERTIFICATE-----
```



Wenn Sie für ePolicy Orchestrator ein signiertes Zertifikat von einem Drittanbieter (z. B. VeriSign oder Microsoft Windows Enterprise Certificate Authority) erstellen lassen möchten, finden Sie Informationen dazu im KnowledgeBase-Artikel KB72477.

4 Informationen über das Hochladen und Verwalten des Zertifikats auf dem ePolicy Orchestrator-Server finden Sie unter *Konfigurieren von ePolicy Orchestrator für die zertifikatbasierte Authentifizierung*.

Weitere nützliche OpenSSL-Befehle

Sie können weitere OpenSSL-Befehle verwenden, um die in PKCS12-Zertifikaten generierten Schlüssel zu extrahieren sowie zu kombinieren, und um eine kennwortgeschützte private Schlüssel-PEM-Datei in eine nicht kennwortgeschützte Datei umzuwandeln.

Befehle für die Verwendung mit PKCS12-Zertifikaten

Mit den folgenden Befehlen können Sie ein PKCS12-Zertifikat erstellen, bei dem sich sowohl das Zertifikat als auch der Schlüssel in einer einzigen Datei befinden.

Beschreibung	OpenSSL-Befehlsformat
Erstellt ein Zertifikat und einen Schlüssel in der gleichen Datei.	openssl req -x509 -nodes -days 365 -newkey rsa:1024 -config *Pfad*\openssl.cnf -keyout *Pfad*\pkcs12Example.pem -out *Pfad*\pkcs12Example.pem
Exportiert die PKCS12-Version des Zertifikats.	openssl pkcs12 -export -out *Pfad*\pkcs12Example.pfx -in *Pfad*\pkcs12Example.pem -name "*Benutzername*"

Mit den folgenden Befehlen können Sie das Zertifikat und den Schlüssel aus einem kombinierten PKCS12-Zertifikat trennen.

Beschreibung	OpenSSL-Befehlsformat
Extrahiert den PEM-Schlüssel aus der PFX-Datei.	openssl pkcs12 -in pkcs12ExampleKey.pfx -out pkcs12ExampleKey.pem
Entfernt das Kennwort im Schlüssel.	openssl rsa -in pkcs12ExampleKey.pem -out pkcs12ExampleKeyNoPW.pem ePolicy Orchestrator kann die Datei "pkcs12ExampleCert.pem" als Zertifikat und die Datei "pkcs12ExampleKey.pem" als Schlüssel verwenden (oder den Schlüssel ohne Kennwort "pkcs12ExampleKeyNoPW.pem").

Befehl zum Umwandeln einer kennwortgeschützten privaten Schlüssel-PEM-Datei

Geben Sie den folgenden Befehl ein, um eine kennwortgeschützte private Schlüssel-PEM-Datei in eine nicht kennwortgeschützte Datei umzuwandeln:

```
openssl rsa -in C:\ssl\keys\key.pem -out C:\ssl\keys\keyNoPassword.pem
```



Im vorherigen Beispiel steht "C:\ssl\keys" für den Eingabe- und den Ausgabepfad für die Dateien "key.pem" und "keyNoPassword.pem".

Konvertieren einer vorhandenen PVK-Datei in eine PEM-Datei

Der ePolicy Orchestrator-Browser unterstützt PEM-codierte private Schlüssel. Dazu gehören sowohl kennwortgeschützte als auch nicht durch Kennwörter geschützte private Schlüssel. Mithilfe von OpenSSL können Sie einen Schlüssel aus dem PVK- in das PEM-Format konvertieren.

Bevor Sie beginnen

Zum Konvertieren der PVK-Datei müssen Sie OpenSSL für Windows installieren. Diese Software ist unter der folgenden URL-Adresse verfügbar:

http://www.slproweb.com/products/Win32OpenSSL.html

Konvertieren Sie Ihr Zertifikat mithilfe von OpenSSL für Windows aus dem PVK- in das PEM-Format.

Vorgehensweise

1. Geben Sie den folgenden Befehl in der Befehlszeile ein, um eine zuvor erstellte PVK-Datei in eine PEM-Datei zu konvertieren:

   ```
   openssl rsa -inform PVK -outform PEM -in C:\ssl\keys\myPrivateKey.pvk -out C:\ssl
   \keys\myPrivateKey.pem -passin pass:p@$$w0rd -passout pass:p@$$w0rd
   ```

   Die Argumente "-passin" und "-passout" im oben gezeigten Befehl sind optional.

2. Wenn Sie dazu aufgefordert werden, geben Sie das Kennwort ein, mit dem Sie die PKV-Datei erstellt haben.

   Wenn das Argument "-passout" im oben gezeigten Beispiel nicht verwendet wird, ist der neu erstellte Schlüssel im PEM-Format nicht kennwortgeschützt.

Berechtigungssätze

Mit Berechtigungssätzen wird die Ebene des Zugriffs kontrolliert, den Benutzer auf in der Software verfügbare Funktionen haben.

Selbst in der kleinsten ePolicy Orchestrator-Installation muss der Zugriff festgelegt und kontrolliert werden, den Benutzer auf die verschiedenen Teile des Systems haben.

Inhalt

Das Zusammenspiel von Benutzern, Gruppen und Berechtigungssätzen

Der Zugriff auf Elemente in ePolicy Orchestrator wird durch das Zusammenspiel von Benutzern, Gruppen und Berechtigungssätzen gesteuert.

Benutzer

Es gibt zwei allgemeine Kategorien von Benutzern: die Administratoren, die volle Rechte im System haben, und die normalen Benutzer. Normalen Benutzern kann eine beliebige Anzahl von Berechtigungssätzen zugewiesen werden, die deren Zugriffsebenen in ePolicy Orchestrator definieren.

Benutzerkonten können auf verschiedene Weisen erstellt und verwaltet werden. Folgende Möglichkeiten stehen zur Verfügung:

- Sie können Benutzerkonten manuell erstellen und dann jedem Konto einen geeigneten Berechtigungssatz zuweisen.
- Sie können den ePolicy Orchestrator-Server so konfigurieren, dass sich Benutzer mittels Windows-Authentifizierung anmelden können.

Das Zulassen von Benutzeranmeldungen mithilfe von Windows-Anmeldeinformationen ist eine erweiterte Funktion, für die mehrere Einstellungen und Komponenten konfiguriert bzw. eingerichtet werden müssen. Weitere Informationen zu dieser Möglichkeit finden Sie unter *Verwalten von ePolicy Orchestrator-Benutzern mit Active Directory*.

Auch wenn Benutzerkonten und Berechtigungssätze in einer engen Beziehung zueinander stehen, werden sie auf unterschiedliche Weise erstellt und konfiguriert. Weitere Informationen zu Berechtigungssätzen finden Sie unter *Verwalten von Berechtigungssätzen*.

Administratoren

Administratoren besitzen die Berechtigung zum Lesen und Schreiben sowie zum Ausführen aller Vorgänge. Beim Installieren des Servers wird automatisch ein Administratorkonto erstellt. In der Standardeinstellung lautet der Benutzername für dieses Konto **admin**. Wenn der Standardwert während der Installation geändert wird, wird dieses Konto entsprechend umbenannt.

Sie können für Benutzer, die Administratorrechte benötigen, weitere Administratorkonten erstellen.

Zu den Berechtigungen, die nur Administratoren vorbehalten sind, gehören die folgenden:

- Erstellen, Bearbeiten und Löschen von Quellsites und alternativen Sites
- Ändern von Server-Einstellungen
- Hinzufügen und Löschen von Benutzerkonten

- Hinzufügen, Löschen und Zuweisen von Berechtigungssätzen
- Importieren von Ereignissen in ePolicy Orchestrator-Datenbanken und Einschränken der Ereignisse, die dort gespeichert werden

Gruppen

Den Gruppen werden Abfragen und Berichte zugewiesen. Eine Gruppe kann privat (nur für den jeweiligen Benutzer), global öffentlich ("freigegeben") oder für ein oder mehrere Berechtigungssätze freigegeben sein.

Berechtigungssätze

In einem Berechtigungssatz wird ein bestimmtes Zugriffsprofil definiert. Das beinhaltet meist eine Kombination von Zugriffsebenen für verschiedene Teile von ePolicy Orchestrator. So kann zum Beispiel ein einzelner Berechtigungssatz die Erlaubnis zum Lesen des Audit-Protokolls, zum Verwenden öffentlicher und freigegebener Dashboards sowie zum Erstellen und Bearbeiten öffentlicher Berichte und Abfragen erteilen.

Berechtigungssätze können einzelnen Benutzern oder – bei Verwendung von Active Directory – allen Benutzern von bestimmten Active Directory-Servern zugewiesen werden.

Arbeiten mit Berechtigungssätzen

Auf der Seite **Berechtigungssätze** können Sie den Benutzerzugriff steuern und Berechtigungssätze erstellen sowie ändern.

Aufgaben

- *Verwalten von Berechtigungssätzen* auf Seite 55
  Auf der Seite **Berechtigungssätze** können Sie den Benutzerzugriff steuern und Berechtigungssätze erstellen, ändern, exportieren sowie importieren.
- *Exportieren und Importieren von Berechtigungssätzen* auf Seite 57
  Nachdem Sie Ihre Berechtigungssätze fertig definiert haben, können diese am einfachsten auf andere McAfee ePO-Server migriert werden, indem Sie sie auf die anderen Server exportieren.

Verwalten von Berechtigungssätzen

Auf der Seite **Berechtigungssätze** können Sie den Benutzerzugriff steuern und Berechtigungssätze erstellen, ändern, exportieren sowie importieren.



Nachdem Sie Ihre Berechtigungssätze fertig definiert haben, können diese am einfachsten auf andere ePolicy Orchestrator-Server migriert werden, indem Sie sie exportieren und auf den anderen Servern importieren.

Vorgehensweise

Definitionen zu Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

1. Klicken Sie zum Öffnen der Seite **Berechtigungssätze** auf **Menü** | **Benutzerverwaltung** | **Berechtigungssätze**.
2. Wählen Sie eine der folgenden Aktionen aus.

Aktion	**Vorgehensweise**
Erstellen eines neuen Berechtigungssatzes	1 Klicken Sie auf **Aktionen | Neu**. 2 Geben Sie einen Namen für den neuen Berechtigungssatz ein. Die Verwendung eines bereits vorhandenen Namens ist in ePolicy Orchestrator nicht erlaubt. Jeder Berechtigungssatz muss einen eindeutigen Namen besitzen. 3 Wenn Sie diesem Berechtigungssatz sofort bestimmte Benutzer zuweisen möchten, wählen Sie die Namen der gewünschten Benutzer im Abschnitt **Benutzer** aus. 4 Wenn Active Directory-Gruppen vorhanden sind, aus denen alle Benutzer dem Berechtigungssatz zugeordnet werden sollen, wählen Sie den Server in der Liste **Server-Name** aus, und klicken Sie auf **Hinzufügen**. 5 Wenn Sie Active Directory-Server hinzugefügt haben, die Sie entfernen möchten, wählen Sie die gewünschten Server im Listenfeld **Active Directory** aus, und klicken Sie auf **Entfernen**. 6 Klicken Sie zum Speichern des Berechtigungssatzes auf **Speichern**. Der Berechtigungssatz ist nun erstellt, ihm sind jedoch noch keine Berechtigungen zugewiesen.
Ändern eines vorhandenen Berechtigungssatzes	1 Wählen Sie den zu ändernden Berechtigungssatz aus. Detaillierte Informationen zu diesem Berechtigungssatz werden rechts angezeigt. Falls Sie gerade einen neuen Berechtigungssatz erstellt haben, ist dieser bereits ausgewählt. 2 Wählen Sie eine Kategorie von zu ändernden Berechtigungen aus, indem Sie in der Zeile dieser Kategorie auf **Bearbeiten** klicken. Die für die ausgewählte Berechtigungskategorie verfügbaren Optionen werden angezeigt. 3 Nehmen Sie an den Berechtigungen die gewünschten Änderungen vor, und klicken Sie dann auf **Speichern**. Dadurch werden die Änderungen an dem Berechtigungssatz in die Datenbank übernommen. Wenn Sie den Berechtigungssatz fertig geändert haben, brauchen Sie zum Abschluss nicht auf **Speichern** zu klicken. Die Änderungen werden direkt beim Ändern der jeweiligen Kategorie gespeichert. Zudem werden die vorgenommenen Änderungen sofort im System übernommen und gemäß Ihrer Richtlinienkonfiguration im restlichen Netzwerk verbreitet.
Duplizieren von Berechtigungssätzen	1 Wählen Sie den Berechtigungssatz, den Sie duplizieren möchten, in der Liste **Berechtigungssätze** aus, und klicken Sie auf **Aktionen | Duplizieren**. 2 Geben Sie einen neuen Namen für den duplizierten Berechtigungssatz ein. In der Standardeinstellung hängt ePolicy Orchestrator den Hinweis (Kopie) an den vorhandenen Namen an. Die Verwendung eines bereits vorhandenen Namens ist in ePolicy Orchestrator nicht erlaubt. Jeder Berechtigungssatz muss einen eindeutigen Namen besitzen. 3 Klicken Sie auf **OK**. Der Berechtigungssatz ist jetzt dupliziert, in der Liste **Berechtigungssätze** ist jedoch immer noch das Original ausgewählt.

Aktion	Vorgehensweise
Löschen von Berechtigungssätzen	1 Wählen Sie den Berechtigungssatz aus, den Sie in der Liste **Berechtigungssätze** löschen möchten. Detaillierte Informationen zu diesem Berechtigungssatz werden rechts angezeigt. 2 Klicken Sie auf **Aktionen** | **Löschen**, und klicken Sie im Bereich **Aktion** auf **OK**. Der Berechtigungssatz wird nun nicht mehr in der Liste **Berechtigungssätze** angezeigt.
Exportieren von Berechtigungssätzen	1 Wählen Sie die zu exportierenden Berechtigungssätze aus. 2 Klicken Sie auf **Aktionen für Berechtigungssätze** | **Alle exportieren**. Der McAfee ePO-Server sendet eine XML-Datei an Ihren Browser. Der nächste Schritt hängt von Ihren Browser-Einstellungen ab. Von den meisten Browsern werden Sie standardmäßig zum Speichern der Datei aufgefordert. Die XML-Datei enthält nur Rollen mit einigen definierten Berechtigungsebenen. Wenn zum Beispiel ein bestimmter Berechtigungssatz über keine Berechtigungen für Abfragen und Berichte verfügt, enthält die Datei keinen Eintrag.
Importieren von Berechtigungssätzen	1 Wählen Sie die zu importierenden Berechtigungssätze aus. 2 Klicken Sie auf **Durchsuchen**, und wählen Sie die XML-Datei aus, in der sich der zu importierende Berechtigungssatz befindet. 3 Wählen Sie anhand der entsprechenden Option aus, ob Sie Berechtigungssätze, die denselben Namen wie importierte Berechtigungssätze haben, beibehalten möchten oder nicht. Klicken Sie auf **OK**. Wenn ePolicy Orchestrator in der angegebenen Datei keinen gültigen Berechtigungssatz findet, wird eine Fehlermeldung angezeigt, und der Importvorgang wird abgebrochen. Die Berechtigungssätze werden zum Server hinzugefügt und in der Liste **Berechtigungssätze** angezeigt.

Exportieren und Importieren von Berechtigungssätzen

Nachdem Sie Ihre Berechtigungssätze fertig definiert haben, können diese am einfachsten auf andere McAfee ePO-Server migriert werden, indem Sie sie auf die anderen Server exportieren.

Vorgehensweise

Definitionen zu Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

1. Klicken Sie zum Öffnen der Seite **Berechtigungssätze** auf **Menü** | **Benutzerverwaltung** | **Berechtigungssätze**.
2. Wählen Sie eine der folgenden Aktionen aus.

Aktion	Vorgehensweise
Exportieren von Berechtigungssätzen	1 Wählen Sie die zu exportierenden Berechtigungssätze aus. 2 Klicken Sie auf **Aktionen für Berechtigungssätze | Alle exportieren**. Der McAfee ePO-Server sendet eine XML-Datei an Ihren Browser. Der nächste Schritt hängt von Ihren Browser-Einstellungen ab. Von den meisten Browsern werden Sie standardmäßig zum Speichern der Datei aufgefordert. Die XML-Datei enthält nur Rollen mit einigen definierten Berechtigungsebenen. Wenn zum Beispiel ein bestimmter Berechtigungssatz über keine Berechtigungen für Abfragen und Berichte verfügt, enthält die Datei keinen Eintrag.
Importieren von Berechtigungssätzen	1 Wählen Sie die zu importierenden Berechtigungssätze aus. 2 Klicken Sie auf **Durchsuchen**, und wählen Sie die XML-Datei aus, in der sich der zu importierende Berechtigungssatz befindet. 3 Wählen Sie anhand der entsprechenden Option aus, ob Sie Berechtigungssätze, die denselben Namen wie importierte Berechtigungssätze haben, beibehalten möchten oder nicht. Klicken Sie auf **OK**. Wenn ePolicy Orchestrator in der angegebenen Datei keinen gültigen Berechtigungssatz findet, wird eine Fehlermeldung angezeigt, und der Importvorgang wird abgebrochen. Die Berechtigungssätze werden zum Server hinzugefügt und in der Liste **Berechtigungssätze** angezeigt.

6 Repositories

Auf Repositories befinden sich Sicherheits-Software-Pakete sowie deren Aktualisierungen zur Verteilung an die verwalteten Systeme.

Sicherheits-Software ist nur so effektiv wie die zuletzt installierten Aktualisierungen. Wenn zum Beispiel die DAT-Dateien veraltet sind, kann die beste Antiviren-Software keine neuen Bedrohungen erkennen. Es ist wichtig, eine zuverlässige Aktualisierungsstrategie zu entwickeln, damit die Sicherheits-Software immer so aktuell wie möglich ist.

Die Repository-Architektur von ePolicy Orchestrator bietet die Flexibilität, die erforderlich ist, damit das Ausbringen und Aktualisieren von Software so einfach und automatisch erfolgen kann, wie dies die jeweilige Umgebung zulässt. Erstellen Sie nach dem Einrichten der Repository-Infrastruktur Aktualisierungs-Tasks, die bestimmen, wie, wo und wann Ihre Software aktualisiert wird.

Inhalt

Repository-Typen und ihre Funktion

ePolicy Orchestrator stellt verschiedene Typen von Repositories bereit, mit denen sich eine robuste Infrastruktur für Aktualisierungen aufbauen lässt, über die Produkte und Aktualisierungen im gesamten Netzwerk verteilt werden können. Dank dieser Repositories können Sie ganz flexibel eine Aktualisierungsstrategie entwickeln, die sicherstellen soll, dass Ihre Systeme immer auf dem aktuellen Stand sind.

Master-Repository

Im Master-Repository werden die neuesten Versionen der Sicherheits-Software und Aktualisierungen für Ihre Umgebung verwaltet. Dieses Repository stellt die Quelle für den Rest der Umgebung dar.



Standardmäßig verwendet ePolicy Orchestrator die Proxyeinstellungen von Microsoft Internet Explorer.

Verteilte Repositories

In verteilten Repositories sind Kopien der Master-Repository-Inhalte gespeichert. Sie sollten verteilte Repositories verwenden und diese strategisch günstig im gesamten Netzwerk verteilen, um so sicherzustellen, dass verwaltete Systeme auch dann aktualisiert werden, wenn insbesondere über langsame Verbindungen nur minimaler Netzwerkverkehr möglich ist.

Beim Aktualisieren des Master-Repositorys repliziert ePolicy Orchestrator die Inhalte in die verteilten Repositories.

Eine Replizierung kann bei folgenden Gelegenheiten stattfinden:

- Automatisch, wenn festgelegte Pakettypen in das Master-Repository eingecheckt werden und dabei die globale Aktualisierung aktiviert ist
- Regelmäßig, beim geplanten Replizieren mit Replizierungs-Tasks
- Manuell, durch Ausführen des Tasks "Jetzt replizieren"

In einem großen Unternehmen kann es mehrere Standorte geben, die über Leitungen mit begrenzter Bandbreite miteinander verbunden sind. Verteilte Repositories tragen dazu bei, den Aktualisierungsverkehr über Leitungen mit niedrigerer Bandbreite oder an Remote-Standorten mit einer großen Anzahl von Client-Systemen zu reduzieren. Wenn Sie an einem Remote-Standort ein verteiltes Repository erstellen und die Systeme an diesem Standort so konfigurieren, dass sie Aktualisierungen von diesem verteilten Repository abrufen, werden die Aktualisierungen nicht an alle Systeme am Remote-Standort einzeln, sondern nur einmal (nämlich an das verteilte Repository) über die langsame Verbindung kopiert.

Wenn die globale Aktualisierung aktiviert wurde, aktualisieren verteilte Repositories verwaltete Systeme automatisch, sobald bestimmte Aktualisierungen und Pakete in das Master-Repository eingecheckt wurden. Aktualisierungs-Tasks sind nicht erforderlich. Für eine automatische Aktualisierung müssen in Ihrer Umgebung allerdings SuperAgents ausgeführt werden. Außerdem müssen Sie weiterhin Repositories und die Aktualisierungs-Tasks erstellen und konfigurieren.



Wenn verteilte Repositories so eingerichtet sind, dass nur ausgewählte Pakete repliziert werden, wird Ihr neu eingechecktes Paket standardmäßig repliziert. Wenn ein neu eingechecktes Paket nicht repliziert werden soll, müssen Sie dessen Markierung in jedem verteilten Repository aufheben oder den Replizierungs-Task deaktivieren, bevor das Paket eingecheckt wird. Weitere Informationen finden Sie unter *Vermeiden der Replizierung von ausgewählten Paketen* und *Deaktivieren der Replizierung von ausgewählten Paketen*.



Konfigurieren Sie verteilte Repositories nicht so, dass sie auf dasselbe Verzeichnis verweisen wie Ihr Master-Repository. Ansonsten werden die Dateien auf dem Master-Repository durch Benutzer des verteilten Repositorys gesperrt, wodurch Abrufe und das Einchecken von Paketen fehlschlagen können und das Master-Repository nicht mehr verwendbar ist.

Quellsite

Die Quellsite stellt alle Aktualisierungen für Ihr Master-Repository bereit. Die standardmäßige Quellsite ist die McAfeeHttp-Aktualisierungssite. Sie können die Quellsite jedoch auch ändern oder bei Bedarf mehrere Quellsites konfigurieren. Es wird empfohlen, die McAfeeHttp- oder McAfeeFtp-Aktualisierungssite als Quellsite zu verwenden.



Quellsites sind nicht erforderlich. Sie können Aktualisierungen manuell herunterladen und in das Master-Repository einchecken. Wenn Sie eine Quellsite verwenden, wird dieser Vorgang jedoch automatisch durchgeführt.

McAfee veröffentlicht auf diesen Sites regelmäßig Software-Aktualisierungen. DAT-Dateien werden beispielsweise täglich veröffentlicht. Aktualisieren Sie Ihr Master-Repository mit Aktualisierungen, sobald diese verfügbar sind.

Kopieren Sie mithilfe von Abruf-Tasks Inhalte aus einer Quellsite in das Master-Repository.

Auf den McAfee-Aktualisierungssites werden nur Aktualisierungen von Virusdefinitionen (DAT-Dateien) und Scan-Modulen sowie einige Sprachpakete bereitgestellt. Alle anderen Pakete und Aktualisierungen, einschließlich Service Packs und Patches, müssen Sie manuell in Ihr Master-Repository einchecken.

Alternative Site

Die alternative Site ist eine Quellsite, die als Sicherungsmöglichkeit dient, damit verwaltete Systeme Aktualisierungen abrufen können, wenn sie auf ihre eigenen Repositories nicht zugreifen können. Wenn zum Beispiel das Netzwerk ausfällt oder ein Virus ausbricht, lassen sich die standardmäßigen Speicherorte in einigen Fällen nur noch schwierig erreichen. Mithilfe alternativer Sites bleiben verwaltete Systeme jedoch auch in solchen Situationen auf dem aktuellen Stand. Standardmäßig ist die alternative Site die McAfeeHttp-Aktualisierungssite. Sie können nur eine alternative Site aktivieren.

Wenn verwaltete Systeme einen Proxyserver für den Zugriff auf das Internet verwenden, müssen Sie für diese Systeme die Einstellungen der Agenten-Richtlinie so konfigurieren, dass der Zugriff auf diese alternative Site über Proxyserver erfolgt.

Typen verteilter Repositories

ePolicy Orchestrator unterstützt vier Typen verteilter Repositories. Berücksichtigen Sie bei der Entscheidung, welcher Typ verteilter Repositories verwendet werden soll, Ihre Umgebung und Ihren Bedarf. Sie müssen sich nicht auf nur einen Typ beschränken. Je nach Netzwerk müssen Sie möglicherweise mehrere Typen verwenden.

SuperAgent-Repositories

Verwenden Sie Systeme mit SuperAgents als verteilte Repositories. SuperAgent-Repositories weisen gegenüber anderen Typen verteilter Repositories einige Vorteile auf:

- Ordnerpfade werden auf dem Hostsystem automatisch erstellt, bevor das Repository zur Repository-Liste hinzugefügt wird.
- Für SuperAgent-Repositories müssen keine Anmeldeinformationen für Replizierung oder Aktualisierung angegeben werden – die Kontoberechtigungen werden erstellt, wenn der Agent in einen SuperAgent konvertiert wird.



Damit die SuperAgent-Reaktivierung funktioniert, muss sich in jedem Übertragungssegment ein SuperAgent befinden. Für das SuperAgent-Repository ist dies dagegen nicht notwendig. Verwaltete Systeme müssen nur auf das System zugreifen können, auf dem sich das Repository befindet.

FTP-Repositories

Sie können ein verteiltes Repository auf einem FTP-Server speichern. Verwenden Sie eine FTP-Server-Software (z. B. die Microsoft-Internetinformationsdienste, IIS), um einen neuen Ordner und ein neues Siteverzeichnis für das verteilte Repository zu erstellen. Ausführliche Informationen hierzu finden Sie in der Dokumentation zum Web-Server.

HTTP-Repositories

Sie können ein verteiltes Repository auf einem HTTP-Server speichern. Verwenden Sie eine HTTP-Server-Software (z. B. Microsoft IIS), um einen neuen Ordner und ein neues Siteverzeichnis für das verteilte Repository zu erstellen. Ausführliche Informationen hierzu finden Sie in der Dokumentation zum Web-Server.

UNC-Freigabe-Repositories

Sie können einen freigegebenen UNC-Ordner erstellen, um ein verteiltes Repository auf einem vorhandenen Server zu speichern. Sie müssen den Ordner im gesamten Netzwerk freigeben, damit Ihr McAfee ePO-Server Dateien in diesen Ordner kopieren kann und Agenten für Aktualisierungen darauf zugreifen können.



Um auf den Ordner zugreifen zu können, müssen die richtigen Berechtigungen festgelegt sein.

Nicht verwaltete Repositories

Wenn Sie keine verwalteten verteilten Repositories verwenden können, können ePolicy Orchestrator-Administratoren verteilte Repositories erstellen und verwalten, die nicht von ePolicy Orchestrator verwaltet werden.

Wenn ein verteiltes Repository nicht von ePolicy Orchestrator verwaltet wird, muss ein lokaler Administrator die verteilten Dateien manuell auf dem aktuellen Stand halten.

Nachdem das verteilte Repository erstellt wurde, können Sie mit ePolicy Orchestrator verwaltete Systeme einer bestimmten Systemstrukturgruppe so konfigurieren, dass sie von dort Aktualisierungen abrufen.



Weitere Informationen zur Konfiguration von nicht verwalteten Systemen für die Verwendung mit ePO finden Sie unter *Aktivieren des Agenten auf nicht verwalteten McAfee-Produkten*.



Sie sollten alle verteilten Repositories über ePolicy Orchestrator verwalten. Dadurch und durch den häufigen Einsatz von globaler Aktualisierung oder geplanten Replizierungs-Tasks wird die Aktualität Ihrer verwalteten Umgebung gewährleistet. Nicht verwaltete verteilte Repositories sollten Sie nur dann verwenden, wenn verwaltete verteilte Repositories in Ihrem Netzwerk oder laut den Richtlinien Ihres Unternehmens nicht zulässig sind.

Repository-Zweige und ihre Verwendung

Mithilfe der drei ePolicy Orchestrator-Repository-Zweige können Sie bis zu drei Versionen der Pakete im Master-Repository und in den verteilten Repositories führen.

Die Repository-Zweige heißen **Aktuell**, **Vorherige** und **Test**. Standardmäßig verwendet ePolicy Orchestrator nur den Zweig **Aktuell**. Sie können Zweige festlegen, wenn Sie Pakete zum Master-Repository hinzufügen. Das Festlegen von Zweigen ist möglich, wenn Sie Aktualisierungs- und Ausbringungs-Tasks durchführen oder planen, um verschiedene Versionen an unterschiedliche Punkte im Netzwerk zu verteilen.

Aktualisierungs-Tasks können Aktualisierungen aus allen Zweigen des Repositorys abrufen. Beim Einchecken von Paketen in das Master-Repository müssen Sie jedoch einen anderen Zweig als **Aktuell** auswählen. Falls nur der Zweig **Aktuell** konfiguriert ist, wird die Option zur Auswahl eines anderen Zweigs als **Aktuell** nicht angezeigt.

Um die Zweige **Test** und **Vorherige** für andere Pakete als Aktualisierungen verwenden zu können, müssen Sie die entsprechenden Server-Einstellungen für die Pakete im Repository konfigurieren. Die Agenten-Versionen 3.6 und früher können nur Aktualisierungspakete aus den Zweigen **Test** und **Vorherige** abrufen.

Zweig "Aktuell"

Der Zweig **Aktuell** ist der Repository-Hauptzweig für die neuesten Pakete und Aktualisierungen. Sofern keine Unterstützung für andere Zweige aktiviert wurde, können Produktausbringungspakete nur zum Zweig **Aktuell** hinzugefügt werden.

Zweig "Test"

Es kann sinnvoll sein, neue DAT- und Scan-Modul-Aktualisierungen vor ihrer Ausbringung im gesamten Unternehmen mit einer kleinen Anzahl von Netzwerksegmenten oder Systemen zu testen. Geben Sie den Zweig **Test** an, wenn Sie neue DAT- und Scan-Modul-Dateien in das Master-Repository einchecken, und bringen Sie sie dann auf einer kleinen Anzahl von Testsystemen aus. Wenn Sie die Testsysteme mehrere Stunden lang überwacht haben, können Sie die neuen DAT-Dateien zum Zweig **Aktuell** hinzufügen und im gesamten Unternehmen ausbringen.

Zweig "Vorherige"

Verwenden Sie den Zweig **Vorherige**, um die vorherigen DAT- und Scan-Modul-Dateien zu sichern und zu speichern, bevor Sie neue zum Zweig **Aktuell** hinzufügen. Falls es in Ihrer Umgebung zu Problemen mit den neuen DAT- oder Scan-Modul-Dateien kommen sollte, besitzen Sie in diesem Fall eine Kopie einer vorherigen Version, die Sie bei Bedarf erneut auf den Systemen ausbringen können. ePolicy Orchestrator speichert nur die aktuellste vorherige Version der einzelnen Dateitypen.

Sie können den Zweig **Vorherige** auffüllen, indem Sie beim Hinzufügen neuer Pakete zum Master-Repository die Option **Vorhandenes Paket in den Zweig 'Vorherige' verschieben** auswählen. Die Option ist verfügbar, wenn Sie Aktualisierungen von einer Quellsite abrufen, und wenn Sie Pakete manuell in den Zweig **Aktuell** einchecken.

Repository-Listen-Datei und ihre Verwendung

Die Repository-Listen-Datei (SITELIST.XML und SITEMGR.XML) enthält die Namen aller Repositories, die Sie verwalten.

Die Repository-Liste enthält den Speicherort und die verschlüsselten Netzwerk-Anmeldeinformationen, die verwaltete Systeme verwenden, um das Repository auszuwählen und Aktualisierungen abzurufen. Der Server sendet die Repository-Liste während einer Agenten-Server-Kommunikation an den Agenten.

Falls erforderlich, können Sie die Repository-Liste in externe Dateien exportieren (SITELIST.XML oder SITEMGR.XML).

Mit einer exportierten Datei SITELIST.XML können Sie folgende Aufgaben durchführen:

- Importieren in einen Agenten während der Installation

Mit einer exportierten Datei SITEMGR.XML können Sie folgende Aufgaben durchführen:

- Sichern und Wiederherstellen verteilter Repositories und Quellsites, wenn der Server neu installiert werden muss
- Importieren der verteilten Repositories und Quellsites aus einer vorherigen Installation von ePolicy Orchestrator

Zusammenarbeit von Repositories

Die Repositories in Ihrer Umgebung arbeiten zusammen, um Aktualisierungen und Software auf die verwalteten Systeme zu übertragen. Je nach der Größe und geografischen Verteilung Ihres Netzwerks benötigen Sie möglicherweise verteilte Repositories.

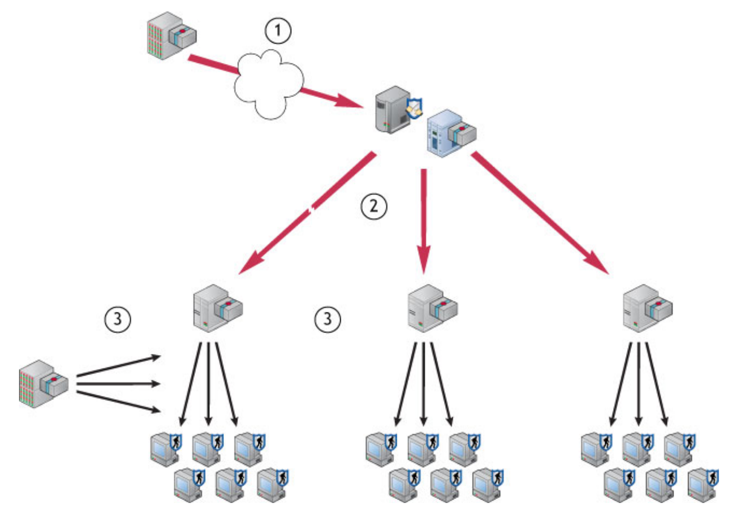


Abbildung 6-1 Sites und Repositories, die Pakete an Systeme verteilen

1. Das Master-Repository ruft regelmäßig DAT- und Scan-Modul-Dateien aus der Quellsite ab.
2. Das Master-Repository repliziert die Pakete in verteilte Repositories im Netzwerk.
3. Die verwalteten Systeme im Netzwerk rufen Aktualisierungen aus einem verteilten Repository ab. Wenn verwaltete Systeme nicht auf verteilte Repositories oder das Master-Repository zugreifen können, rufen sie Aktualisierungen aus der alternativen Site ab.

Erstmaliges Einrichten von Repositories

Gehen Sie wie nachfolgend allgemein beschrieben vor, wenn Sie Repositories zum ersten Mal erstellen.

1. Entscheiden Sie, welche Repository-Typen verwendet werden und wo sich diese befinden sollen.
2. Erstellen Sie die Repositories, und füllen Sie sie auf.

Verwalten von Quellsites und alternativen Sites

In den **Server-Einstellungen** können Sie die standardmäßigen Quellsites und alternativen Sites ändern. So können Sie beispielsweise Einstellungen bearbeiten, vorhandene Quellsites und alternative Sites löschen oder zwischen diesen wechseln.



Um eine Quellsite oder alternative Site definieren, ändern oder löschen zu können, müssen Sie als Administrator angemeldet sein oder die entsprechenden Berechtigungen besitzen.

McAfee empfiehlt, die standardmäßigen Quellsites und alternativen Sites zu verwenden. Wenn Sie hierfür andere Sites benötigen, können Sie neue erstellen.

Erstellen von Quellsites

Sie können unter **Server-Einstellungen** eine neue Quellsite erstellen.

Vorgehensweise

Definitionen zu Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

1. Klicken Sie auf **Menü** | **Konfiguration** | **Server-Einstellungen**, und wählen Sie dann **Quellsites** aus.
2. Klicken Sie auf **Quellsite hinzufügen**. Der Assistent **Quellsite-Generator** wird angezeigt.
3. Geben Sie auf der Seite **Beschreibung** einen eindeutigen Repository-Namen ein, wählen Sie **HTTP**, **UNC** oder **FTP** aus, und klicken Sie dann auf **Weiter**.
4. Geben Sie auf der Seite **Server** die Web-Adress- und Portinformationen der Site an, und klicken Sie dann auf **Weiter**.

   Bei HTTP- oder FTP-Servern:

   - Wählen Sie in der Liste **URL** als Typ der Server-Adresse den Eintrag **DNS-Name**, **IPv4** oder **IPv6** aus, und geben Sie dann die Adresse ein.

Option	Definition
DNS-Name	Gibt den DNS-Namen des Servers an.
IPv4	Gibt die IPv4-Adresse des Servers an.
IPv6	Gibt die IPv6-Adresse des Servers an.

   - Geben Sie die Portnummer des Servers ein: Bei FTP ist dies standardmäßig 21. Bei HTTP ist dies 80.

   Bei UNC-Servern:

   - Geben Sie den Pfad zu dem Netzwerkverzeichnis ein, in dem sich das Repository befindet. Verwenden Sie das folgende Format: `\\<COMPUTER>\<ORDNER>`.

5. Geben Sie auf der Seite **Anmeldeinformationen** die **Anmeldeinformationen zum Herunterladen** an, mit denen verwaltete Systeme eine Verbindung zu diesem Repository herstellen.

   Verwenden Sie Anmeldeinformationen, die nur schreibgeschützten Zugriff auf den HTTP-Server, FTP-Server oder die UNC-Freigabe mit dem Repository gewähren.

   Bei HTTP- oder FTP-Servern:

   - Aktivieren Sie **Anonym**, wenn ein unbekanntes Benutzerkonto verwendet werden soll.
   - Wenn beim Server eine Authentifizierung erforderlich ist, aktivieren Sie **FTP-Authentifizierung** oder **HTTP-Authentifizierung**, und geben Sie dann die Benutzerkontoinformationen ein.

   Bei UNC-Servern:

   - Geben Sie die Domäne und die Benutzerkontoinformationen ein.

6. Klicken Sie auf **Anmeldeinformationen testen**. Nach wenigen Sekunden wird eine Meldung mit der Bestätigung angezeigt, dass Systeme, die die Authentifizierungsinformationen verwenden, auf die Site zugreifen können. Wenn die Anmeldeinformationen falsch sind, überprüfen Sie Folgendes:
   - Benutzername und Kennwort
   - URL-Adresse oder Pfad im vorherigen Fenster des Assistenten
   - HTTP-, FTP oder UNC-Site des Systems
7. Klicken Sie auf **Weiter**.
8. Überprüfen Sie die Angaben auf der Seite **Zusammenfassung**, und klicken Sie dann auf **Speichern**, um die Site zur Liste hinzuzufügen.

Wechseln zwischen Quellsites und alternativen Sites

Verwenden Sie die **Server-Einstellungen**, wenn Sie zwischen Quellsites und alternativen Sites wechseln möchten.

Je nach Ihrer Netzwerkkonfiguration möchten Sie vielleicht zwischen Quellsite und alternativer Site umschalten, wenn Sie feststellen, dass die HTTP- oder die FTP-Aktualisierung besser funktioniert.

Definitionen zu Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

Vorgehensweise

1. Klicken Sie auf **Menü** | **Konfiguration** | **Server-Einstellungen**.
2. Wählen Sie **Quellsites** aus, und klicken Sie dann auf **Bearbeiten**. Die Seite **Quellsites: Bearbeiten** wird angezeigt.
3. Suchen Sie in der Liste die Site, die Sie als alternative Site festlegen möchten, und klicken Sie dann auf **Alternative aktivieren**.

Bearbeiten von Quellsites und alternativen Sites

In den **Server-Einstellungen** können Sie die Einstellungen (wie URL-Adresse, Portnummer, Authentifizierungs-Anmeldeinformationen zum Herunterladen) von Quellsites oder alternativen Sites bearbeiten.

Definitionen zu Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

Vorgehensweise

1. Klicken Sie auf **Menü** | **Konfiguration** | **Server-Einstellungen**.
2. Wählen Sie **Quellsites** aus, und klicken Sie dann auf **Bearbeiten**. Die Seite **Quellsites: Bearbeiten** wird angezeigt.
3. Suchen Sie die Site in der Liste, und klicken Sie auf den Namen der Site.

   Der **Quellsite-Generator** wird angezeigt.
4. Bearbeiten Sie die im Assistenten angezeigten Einstellungen nach Bedarf, und klicken Sie dann auf **Speichern**.

Löschen von Quellsites oder Deaktivieren alternativer Sites

Wenn eine Quellsite oder eine alternative Site nicht mehr benötigt wird, können Sie sie löschen oder deaktivieren.

Definitionen zu Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

Vorgehensweise

1. Klicken Sie auf **Menü** | **Konfiguration** | **Server-Einstellungen**.
2. Wählen Sie **Quellsites** aus, und klicken Sie dann auf **Bearbeiten**. Die Seite **Quellsites: Bearbeiten** wird angezeigt.
3. Klicken Sie neben der erforderlichen Quellsite auf **Löschen**. Das Dialogfeld **Quellsite löschen** wird angezeigt.
4. Klicken Sie auf **OK**.

Die Site wird von der Seite **Quellsites** gelöscht.

Sicherstellen des Zugriffs auf die Quellsite

Sie müssen sicherstellen, dass das ePolicy Orchestrator-Master-Repository, verwaltete Systeme und der Dashboard-Monitor "McAfee Labs-Sicherheitsbedrohungen" auf das Internet zugreifen können, wenn die Sites "McAfeeHttp" und "McAfeeFTP" als Quellsites und alternative Sites verwendet werden.

In diesem Abschnitt werden die erforderlichen Konfigurationsschritte beschrieben, damit das ePolicy Orchestrator-Master-Repository, McAfee Agent und die McAfee Labs-Sicherheitsbedrohungen direkt oder über einen Proxy eine Verbindung zur Download-Seite herstellen. Standardmäßig ist **Keinen Proxy verwenden** ausgewählt.

Konfigurieren von Proxyeinstellungen

Sie können Proxyeinstellungen für den Abruf von DAT-Dateien konfigurieren, mit denen Sie Ihre Repositories und McAfee Labs-Sicherheitsbedrohungen aktualisieren.

Vorgehensweise

Definitionen zu Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

1. Klicken Sie auf **Menü** | **Konfiguration** | **Server-Einstellungen**.

   Die Seite **Server-Einstellungen** wird angezeigt.

2. Wählen Sie in der Liste **Einstellungskategorien** die Option **Proxyeinstellungen** aus, und klicken Sie dann auf **Bearbeiten**.

   Die Seite **Proxyeinstellungen: Bearbeiten** wird angezeigt.

3. Wählen Sie **Proxyeinstellungen manuell konfigurieren** aus.

4. Wählen Sie neben **Proxyserver-Einstellungen** aus, ob ein Proxyserver für die gesamte Kommunikation oder unterschiedliche Proxyserver als HTTP- und FTP-Proxyserver verwendet werden sollen. Geben Sie dann die IP-Adresse oder den vollqualifizierten Domänennamen und die Portnummer (**Port**) des Proxyservers ein.

   Wenn Sie die standardmäßigen Quell- und alternativen Sites verwenden oder andere HTTP-Quellsites und alternativen FTP-Sites konfigurieren, geben Sie hier sowohl die HTTP- als auch die FTP-Proxy-Authentifizierungsinformationen an.

5. Nehmen Sie neben **Proxyauthentifizierung** die entsprechenden Einstellungen vor, je nach dem, ob Sie Aktualisierungen aus HTTP-, aus FTP-Repositories oder aus beiden abrufen.

6. Aktivieren Sie neben **Ausschlüsse** die Option **Lokale Adressen umgehen**, und legen Sie dann alle verteilten Repositories fest, zu denen der Server direkt eine Verbindung herstellen kann, indem Sie die IP-Adressen oder die vollqualifizierten Domänennamen dieser Systeme eingeben (getrennt durch ein Semikolon).

7. Klicken Sie auf **Speichern**.

Konfigurieren von Proxyeinstellungen für McAfee Agent

Sie können die Proxyeinstellungen konfigurieren, mit denen McAfee Agent eine Verbindung zur Download-Website herstellt.

Vorgehensweise

Definitionen zu Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

1. Klicken Sie auf **Menü** | **Richtlinie** | **Richtlinienkatalog**, und wählen Sie dann in der Dropdown-Liste **Produkt** den Eintrag **McAfee Agent** und in der Dropdown-Liste **Kategorie** den Eintrag **Repository** aus.

   Eine Liste mit den für den McAfee ePO-Server konfigurierten Agenten wird angezeigt.

2. Klicken Sie für den Agenten **My Default** auf **Einstellungen bearbeiten**.

   Die Seite zum Bearbeiten der Einstellungen für den Agenten **My Default** wird angezeigt.

3. Klicken Sie auf die Registerkarte **Proxy**.

   Die Seite **Proxyeinstellungen** wird angezeigt.

4. Wählen Sie die Option **Internet Explorer-Einstellungen verwenden (nur Windows)** für Windows-Systeme und bei Bedarf **Konfigurieren von Proxyeinstellungen durch Benutzer zulassen** aus.

   Internet Explorer kann auf mehrere Arten für die Verwendung mit Proxies konfiguriert werden. McAfee stellt Anweisungen für die Konfiguration und Verwendung von McAfee-Produkten, nicht jedoch für Produkte von anderen Anbietern als McAfee bereit. Weitere Informationen über das Konfigurieren von Proxyeinstellungen finden Sie in der Hilfe zu Internet Explorer und unter http://support.microsoft.com/kb/226473.

5. Wählen Sie **Proxyeinstellungen manuell konfigurieren** aus, um die Proxyeinstellungen für den Agenten manuell zu konfigurieren.

6. Geben Sie die IP-Adresse oder den vollqualifizierten Domänennamen und die Portnummer der HTTP- oder FTP-Quelle ein, von der der Agent Aktualisierungen abruft. Aktivieren Sie **Diese Einstellungen für alle Proxytypen verwenden**, um diese Einstellungen als Standardeinstellung für alle Proxytypen festzulegen.

7. Wählen Sie **Ausnahmen festlegen** aus, um Systeme zu kennzeichnen, die keinen Zugriff auf den Proxy benötigen. Verwenden Sie ein Semikolon, um Ausnahmen voneinander zu trennen.

8. Aktivieren Sie **HTTP-Proxyauthentifizierung verwenden** oder **FTP-Proxyauthentifizierung verwenden**, und geben Sie dann einen Benutzernamen und Anmeldeinformationen an.

9. Klicken Sie auf **Speichern**.

Konfigurieren von Proxyeinstellungen für McAfee Labs-Sicherheitsbedrohungen

Wenn Sie nicht die Standardeinstellungen des ePolicy Orchestrator-Servers verwenden, können Sie Proxyeinstellungen für McAfee Labs-Sicherheitsbedrohungen konfigurieren.

Vorgehensweise

Definitionen zu Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

1. Klicken Sie auf **Menü** | **Konfiguration** | **Server-Einstellungen**.

2. Wählen Sie **Proxyeinstellungen** aus, und klicken Sie auf **Bearbeiten**.

   Die Seite **Proxyeinstellungen: Bearbeiten** wird angezeigt.

3. Wählen Sie **Proxyeinstellungen manuell konfigurieren** aus.

4. Wählen Sie neben **Proxyserver-Einstellungen** aus, ob ein Proxyserver für die gesamte Kommunikation oder unterschiedliche Proxyserver als HTTP- und FTP-Proxyserver verwendet werden sollen. Geben Sie dann die IP-Adresse oder den vollqualifizierten Domänennamen und die Portnummer (**Port**) des Proxyservers ein.

   Wenn Sie die standardmäßigen Quell- und alternativen Sites verwenden oder andere HTTP-Quellsites und alternativen FTP-Sites konfigurieren, geben Sie hier sowohl die HTTP- als auch die FTP-Proxy-Authentifizierungsinformationen an.

5. Nehmen Sie neben **Proxyauthentifizierung** die entsprechenden Einstellungen vor, je nach dem, ob Sie Aktualisierungen aus HTTP-, aus FTP-Repositories oder aus beiden abrufen.

6 Aktivieren Sie neben **Ausschlüsse** die Option **Lokale Adressen umgehen**, und legen Sie dann alle verteilten Repositories fest, zu denen der Server direkt eine Verbindung herstellen kann, indem Sie die IP-Adressen oder die vollqualifizierten Domänennamen dieser Systeme eingeben (getrennt durch Semikolon).

7 Klicken Sie auf **Speichern**.

Konfigurieren von Einstellungen für globale Aktualisierungen

Mit globalen Aktualisierungen können Sie die Repository-Replizierung in Ihrem Netzwerk automatisieren. Nutzen Sie die Server-Einstellung **Globale Aktualisierung**, um die Inhalte zu konfigurieren, die bei einer globalen Aktualisierung an Repositories verteilt werden.

Globale Aktualisierungen sind standardmäßig deaktiviert. McAfee empfiehlt jedoch, dass Sie diese Aktualisierungen aktivieren und im Rahmen Ihrer Aktualisierungsstrategie nutzen. Sie können ein Zufallsintervall und Pakettypen angeben, die während der Aktualisierung verteilt werden sollen. Das Zufallsintervall gibt die Zeitspanne an, in der alle Systeme aktualisiert werden. Innerhalb dieses angegebenen Intervalls werden die Systeme auf Zufallsbasis aktualisiert.

Vorgehensweise

Definitionen zu Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

1 Klicken Sie auf **Menü** | **Konfiguration** | **Server-Einstellungen**, wählen Sie in der Liste **Einstellungskategorien** den Eintrag **Globale Aktualisierung** aus, und klicken Sie dann auf **Bearbeiten**.

2 Legen Sie für den Status **Aktiviert** fest, und geben Sie ein **Zufallsintervall** zwischen 0 und 32.767 Minuten an.

3 Geben Sie an, welche **Pakettypen** in den globalen Aktualisierungen enthalten sein sollen:

- **Alle Pakete** – Bei Auswahl dieser Option werden alle Signaturen und Scan-Module sowie alle Patches und Service Packs in die globalen Aktualisierungen eingeschlossen.
- **Ausgewählte Pakete** – Bei dieser Option können Sie die in globalen Aktualisierungen eingeschlossenen Signaturen und Scan-Module sowie Patches und Service Packs begrenzen.



Wenn Sie die globale Aktualisierung verwenden, empfiehlt McAfee, dass Sie einen regelmäßigen Abruf-Task (zum Aktualisieren des Master-Repositorys) für einen Zeitpunkt planen, zu dem nur wenig Netzwerkverkehr auftritt. Die globale Aktualisierung ist zwar die schnellste Aktualisierungsmethode, verursacht dabei jedoch verstärkten Netzwerkverkehr. Weitere Informationen zum Durchführen globaler Aktualisierungen finden Sie in *Globale Aktualisierung* unter *Ausbringen von Produkten und Aktualisierungen*.

Verwenden von SuperAgents als verteilte Repositories

Sie können auf Systemen, auf denen sich SuperAgents befinden, verteilte Repositories erstellen und konfigurieren. Mithilfe von SuperAgents kann der Netzwerkdatenverkehr minimiert werden.



Damit ein Agent in einen SuperAgent umgewandelt werden kann, muss er zu einer Windows-Domäne gehören.

Erstellen von verteilten SuperAgent-Repositories

Zum Erstellen eines SuperAgent-Repositorys muss auf dem gewünschten System ein McAfee ePO-Agent installiert sein und ausgeführt werden. Sie sollten SuperAgent-Repositories mit aktivierter globaler Aktualisierung verwenden.

Bei dieser Vorgehensweise wird davon ausgegangen, dass Sie wissen, wo sich die gewünschten Systeme in der **Systemstruktur** befinden. Sie sollten ein SuperAgent-Tag erstellen, damit Sie die Systeme mithilfe der Seite **Tag-Katalog** oder durch Ausführen einer Abfrage leicht finden können.

Vorgehensweise

Definitionen zu Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

1. Klicken Sie in der ePO-Konsole auf **Menü** | **Richtlinie** | **Richtlinienkatalog**, und wählen Sie dann in der Dropdown-Liste **Produkt** den Eintrag **McAfee Agent** und in der Dropdown-Liste **Kategorie** den Eintrag **Allgemein** aus.

   Es wird eine Liste mit den Richtlinien der Kategorie **Allgemein** angezeigt, die für Ihren ePolicy Orchestrator-Server zur Verfügung stehen.

2. Erstellen Sie eine neue Richtlinie, duplizieren Sie eine vorhandene Richtlinie, oder öffnen Sie eine vorhandene Richtlinie, die bereits auf Systeme mit einem SuperAgent angewendet wird, auf denen Sie SuperAgent-Repositories hosten möchten.

3. Wählen Sie die Registerkarte **Allgemein** aus, und vergewissern Sie sich, dass die Option **Agenten in SuperAgents konvertieren (nur Windows)** ausgewählt ist.

4. Aktivieren Sie **Systeme mit SuperAgents als verteilte Repositories verwenden**, und geben Sie dann einen Ordnerpfad als Speicherort für das Repository ein. Dies ist der Speicherort, in den das Master-Repository die Aktualisierungen während der Replizierung kopiert. Sie können Standardvariablen von Windows verwenden (z. B. <PROGRAM_FILES_DIR>).

   Alle angeforderten Dateien vom Agenten-System werden aus diesem Speicherort über den integrierten HTTP-Web-Server des Agenten übermittelt.

5. Klicken Sie auf **Speichern**.

6. Weisen Sie diese Richtlinie jedem System zu, das als Host für ein SuperAgent-Repository dienen soll.

Wenn sich der Agent das nächste Mal beim Server meldet, wird die neue Richtlinie abgerufen. Wenn Sie nicht bis zur nächsten Agent-zu-Server-Kommunikation warten möchten, können Sie eine Agenten-Reaktivierung an die Systeme senden. Beim Erstellen des verteilten Repositorys wird der angegebene Ordner auf dem System erstellt, falls dieser nicht bereits vorhanden ist.

Außerdem wird der Speicherort zur Repository-Liste der Datei `SITELIST.XML` hinzugefügt. Auf diese Weise kann die Site von Systemen in der verwalteten Umgebung zum Aktualisieren verwendet werden.

Replizieren von Paketen in SuperAgent-Repositories

Sie können auswählen, welche Repository-spezifischen Pakete in verteilte Repositories repliziert werden.

Definitionen zu Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

Vorgehensweise

1. Klicken Sie auf **Menü** | **Software** | **Verteilte Repositories**.

   Eine Liste aller verteilten Repositories wird angezeigt.

2 Suchen Sie das gewünschte SuperAgent-Repository, und klicken Sie darauf.

Der Assistent **Generator für verteilte Repositories** wird geöffnet.

3 Wählen Sie auf der Seite **Pakettypen** die erforderlichen Pakettypen aus.



Achten Sie darauf, dass alle Pakete ausgewählt sind, die von den verwalteten Systemen benötigt werden, die dieses Repository verwenden. Verwaltete Systeme greifen für alle Pakete auf ein Repository zurück. Wenn ein erwarteter Pakettyp nicht vorhanden ist, kann der Task auf Systemen nicht ausgeführt werden. Diese Funktion stellt sicher, dass Pakete, die nur von wenigen Systemen verwendet werden, nicht in der gesamten Umgebung repliziert werden.

4 Klicken Sie auf **Speichern**.

Löschen von verteilten SuperAgent-Repositories

Sie können verteilte SuperAgent-Repositories aus dem Hostsystem und der Repository-Liste (SITELIST.XML) entfernen. Neue Konfigurationen werden während des nächsten Agent-zu-Server-Kommunikationsintervalls wirksam.

Vorgehensweise

Definitionen zu Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

1 Klicken Sie in der ePolicy Orchestrator-Konsole auf **Menü** | **Richtlinie** | **Richtlinienkatalog**, und klicken Sie dann auf den Namen der SuperAgent-Richtlinie, die Sie ändern möchten.

2 Deaktivieren Sie auf der Registerkarte **Allgemein** die Option **Systeme mit SuperAgents als verteilte Repositories verwenden**, und klicken Sie dann auf **Speichern**.



Um eine begrenzte Anzahl vorhandener verteilter SuperAgent-Repositories zu löschen, duplizieren Sie die diesen Systemen zugewiesene McAfee Agent-Richtlinie, und deaktivieren Sie die Option **Systeme mit SuperAgents als verteilte Repositories verwenden**, bevor Sie sie speichern. Weisen Sie diese neue Richtlinie dann je nach Bedarf zu.

Das SuperAgent-Repository wird gelöscht und aus der Repository-Liste entfernt. Der Agent fungiert jedoch so lange als SuperAgent, bis die Option **Agenten in SuperAgents konvertieren (nur Windows)** deaktiviert wird. Agenten, die nach der Richtlinienänderungen keine neue Sitelist erhalten haben, beziehen ihre Aktualisierungen weiter von dem SuperAgent, der entfernt wurde.

Erstellen und Konfigurieren von Repositories auf FTP- oder HTTP-Servern und UNC-Freigaben

Sie können verteilte Repositories auf vorhandenen FTP- und HTTP-Servern oder UNC-Freigaben hosten. Ein dedizierter Server ist jedoch nicht erforderlich. Das System sollte robust genug sein, um die Lasten zu bewältigen, wenn verwaltete Systeme Verbindungen zum Abrufen von Aktualisierungen herstellen.

Erstellen eines Ordnerspeicherorts

Erstellen Sie den Ordner, der auf dem System mit dem verteilten Repository die Repository-Inhalte enthält. Die Vorgehensweise für UNC-Freigabe-Repositories ist dabei anders als für FTP- oder HTTP-Repositories.

- Für UNC-Freigabe-Repositories erstellen Sie den Ordner auf dem System und aktivieren die Freigabe.
- Für FTP- oder HTTP-Repositories können Sie Ihre vorhandene FTP- oder HTTP-Server-Software (z. B. die Microsoft-Internetinformationsdienste, IIS) verwenden, um einen neuen Ordner und ein neues Siteverzeichnis zu erstellen. Ausführliche Informationen hierzu finden Sie in der Dokumentation zum Web-Server.

Hinzufügen des verteilten Repositorys zu ePolicy Orchestrator

Sie können einen Eintrag zur Repository-Liste hinzufügen und den Ordner angeben, der von dem neuen verteilten Repository verwendet wird.



Konfigurieren Sie verteilte Repositories nicht so, dass sie auf dasselbe Verzeichnis verweisen wie Ihr Master-Repository. Ansonsten werden die Dateien auf dem Master-Repository durch Benutzer des verteilten Repositorys gesperrt, wodurch Abrufe und das Einchecken von Paketen fehlschlagen können und das Master-Repository nicht mehr verwendbar ist.

Vorgehensweise

Definitionen zu Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

1. Klicken Sie auf **Menü** | **Software** | **Verteilte Repositories** und anschließend auf **Aktionen** | **Neues Repository**. Der Assistent **Generator für verteilte Repositories** wird geöffnet.
2. Geben Sie auf der Seite **Beschreibung** einen eindeutigen Namen ein, wählen Sie **HTTP**, **UNC** oder **FTP** aus, und klicken Sie dann auf **Weiter**. Bei dem Namen des Repositorys muss es sich nicht um den Namen des Systems handeln, das als Host für das Repository dient.
3. Konfigurieren Sie auf der Seite **Server** einen der folgenden **Server-Typen**:

   Bei HTTP-Servern:

   - Wählen Sie in der Liste **URL** als Typ der Server-Adresse den Eintrag **DNS-Name**, **IPv4** oder **IPv6** aus, und geben Sie dann die Adresse ein.

Option	Definition
DNS-Name	Gibt den DNS-Namen des Servers an.
IPv4	Gibt die IPv4-Adresse des Servers an.
IPv6	Gibt die IPv6-Adresse des Servers an.

   - Geben Sie die Portnummer des Servers ein: Bei HTTP ist der Standardwert 80.
   - Geben Sie den **UNC-Pfad für die Replizierung** für den HTTP-Ordner an.

   Bei UNC-Servern:

   - Geben Sie den Pfad zu dem Netzwerkverzeichnis ein, in dem sich das Repository befindet. Verwenden Sie das folgende Format: `\\<COMPUTER>\<ORDNER>`.

Bei FTP-Servern:

- Wählen Sie in der Liste **URL** als Typ der Server-Adresse den Eintrag **DNS-Name**, **IPv4** oder **IPv6** aus, und geben Sie dann die Adresse ein.

Option	Definition
DNS-Name	Gibt den DNS-Namen des Servers an.
IPv4	Gibt die IPv4-Adresse des Servers an.
IPv6	Gibt die IPv6-Adresse des Servers an.

- Geben Sie die Portnummer des Servers ein: Bei FTP ist der Standardwert 21.

4 Klicken Sie auf **Weiter**.

5 Gehen Sie auf der Seite **Anmeldeinformationen** wie folgt vor:

a Geben Sie die **Anmeldeinformationen zum Herunterladen** ein. Verwenden Sie Anmeldeinformationen, die nur schreibgeschützten Zugriff auf den HTTP-Server, FTP-Server oder die UNC-Freigabe mit dem Repository gewähren.

Bei HTTP- oder FTP-Servern:

- Aktivieren Sie **Anonym**, wenn ein unbekanntes Benutzerkonto verwendet werden soll.
- Wenn beim Server eine Authentifizierung erforderlich ist, aktivieren Sie **FTP-Authentifizierung** oder **HTTP-Authentifizierung**, und Sie geben dann die Benutzerkontoinformationen ein.

Bei UNC-Servern:

- Wählen Sie **Anmeldeinformationen des angemeldeten Kontos verwenden** aus, um die Anmeldeinformationen des momentan angemeldeten Benutzers zu verwenden.
- Wählen Sie **Geben Sie die Anmeldeinformationen zum Herunterladen ein** aus, und geben Sie die Domänen- und Benutzerkontoinformationen ein.

b Klicken Sie auf **Anmeldeinformationen testen**. Nach wenigen Sekunden wird eine Meldung mit der Bestätigung angezeigt, dass Systeme, die die Authentifizierungsinformationen verwenden, auf die Site zugreifen können. Wenn die Anmeldeinformationen falsch sind, überprüfen Sie Folgendes:

- Benutzername und Kennwort
- URL-Adresse oder Pfad im vorherigen Fenster des Assistenten
- HTTP-, FTP oder UNC-Site des Systems

6 Geben Sie die **Anmeldeinformationen zum Replizieren** ein.

Der Server verwendet diese Anmeldeinformationen beim Replizieren von DAT-Dateien, Scan-Modul-Dateien oder anderen Produktaktualisierungen aus dem Master-Repository in das verteilte Repository. Diese Anmeldeinformationen müssen sowohl Lese- als auch Schreibberechtigungen für das verteilte Repository implizieren.

- Wenn Sie **FTP** ausgewählt haben, geben Sie die Benutzerkontoinformationen ein.
- Wenn Sie **HTTP** oder **UNC** ausgewählt haben, geben Sie die Domänen- und Benutzerkontoinformationen ein.
- Klicken Sie auf **Anmeldeinformationen testen**. Nach wenigen Sekunden wird eine Meldung mit der Bestätigung angezeigt, dass Systeme, die die Authentifizierungsinformationen verwenden, auf

die Site zugreifen können. Wenn die Anmeldeinformationen falsch sind, überprüfen Sie Folgendes:

- Benutzername und Kennwort
- URL-Adresse oder Pfad im vorherigen Fenster des Assistenten
- HTTP-, FTP oder UNC-Site des Systems

7. Klicken Sie auf **Weiter**. Die Seite **Pakettypen** wird angezeigt.
8. Legen Sie fest, ob alle oder nur ausgewählte Pakete in dieses verteilte Repository repliziert werden sollen, und klicken Sie dann auf **Weiter**.
   - Wenn Sie die Option **Ausgewählte Pakete** ausgewählt haben, müssen Sie die zu replizierenden **Signaturen und Scan-Module** sowie **Produkte, Patches, Service Packs etc.** manuell auswählen.
   - Wählen Sie optional **Alte DAT-Dateien replizieren** aus.



Achten Sie darauf, dass alle Pakete aktiviert sind, die von den verwalteten Systemen benötigt werden, die dieses Repository verwenden. Verwaltete Systeme greifen für alle Pakete auf ein Repository zurück. Wenn ein erforderlicher Pakettyp im Repository nicht vorhanden ist, kann der Task nicht ausgeführt werden. Diese Funktion stellt sicher, dass Pakete, die nur von wenigen Systemen verwendet werden, nicht in der gesamten Umgebung repliziert werden.

9. Überprüfen Sie die Angaben auf der Seite **Zusammenfassung**, und klicken Sie dann auf **Speichern**, um das Repository hinzuzufügen. ePolicy Orchestrator fügt das neue verteilte Repository zu seiner Datenbank hinzu.

Vermeiden der Replizierung von ausgewählten Paketen

Wenn verteilte Repositories so eingerichtet sind, dass nur ausgewählte Pakete repliziert werden, wird Ihr neu eingechecktes Paket standardmäßig repliziert. Je nach Ihren Anforderungen in Bezug auf Tests und Überprüfungen möchten Sie möglicherweise vermeiden, dass bestimmte Pakete in Ihre verteilten Repositories repliziert werden.

Gehen Sie wie in dieser Aufgabe beschrieben vor, um die Replizierung eines neu eingecheckten Pakets zu vermeiden.

Vorgehensweise

Definitionen zu Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

1. Klicken Sie auf **Menü** | **Software** | **Verteilte Repositories** und anschließend auf das gewünschte Repository. Der Assistent **Generator für verteilte Repositories** wird geöffnet.
2. Deaktivieren Sie auf der Seite **Pakettypen** das Paket, dessen Replizierung Sie vermeiden möchten.
3. Klicken Sie auf **Speichern**.

Deaktivieren der Replizierung von ausgewählten Paketen

Wenn verteilte Repositories so eingerichtet sind, dass nur ausgewählte Pakete repliziert werden, wird Ihr neu eingechecktes Paket standardmäßig repliziert. Falls Sie die bevorstehende Replizierung eines Pakets deaktivieren möchten, deaktivieren Sie den Replizierungs-Task, bevor Sie das Paket einchecken.

Gehen Sie wie in dieser Aufgabe beschrieben vor, um die Replizierung vor dem Einchecken des neuen Pakets zu deaktivieren.

Vorgehensweise

Definitionen zu Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

1. Klicken Sie auf **Menü** | **Automatisierung** | **Server-Tasks**, und wählen Sie dann neben dem gewünschten Replizierungs-Server-Task die Option **Bearbeiten** aus.

   Daraufhin wird der **Generator für Server-Tasks** angezeigt.

2. Legen Sie auf der Seite **Beschreibung** den **Planungsstatus** auf **Deaktiviert** fest, und klicken Sie dann auf **Speichern**.

Aktivieren der Ordnerfreigabe für UNC- und HTTP-Repositories

Bei einem verteilten HTTP- oder UNC-Repository müssen Sie den Ordner für die Freigabe im Netzwerk aktivieren, damit der ePolicy Orchestrator-Server Dateien in das Repository kopieren kann.

Dies dient nur zu Replizierungszwecken. Verwaltete Systeme, die zum Verwenden des verteilten Repositorys konfiguriert sind, nutzen das entsprechende Protokoll (HTTP, FTP oder Windows-Dateifreigabe) und benötigen keine Ordnerfreigabe.

Vorgehensweise

1. Suchen Sie in Windows Explorer den erstellten Ordner auf dem verwalteten System.

2. Klicken Sie mit der rechten Maustaste auf den Ordner, wählen Sie **Eigenschaften** und dann die Registerkarte **Freigabe** aus.

3. Wählen Sie auf der Registerkarte **Freigabe** die Option **Ordner freigeben** aus.

4. Konfigurieren Sie die Freigabeberechtigungen nach Bedarf.

   Systeme, die über das Repository aktualisiert werden, benötigen nur Lesezugriff, Administratorkonten hingegen (wie das Konto, das vom ePolicy Orchestrator-Server-Dienst verwendet wird) benötigen Schreibzugriff. Informationen zum Konfigurieren der entsprechenden Sicherheitseinstellungen für freigegebene Ordner finden Sie in der Microsoft Windows-Dokumentation.

5. Klicken Sie auf **OK**.

Bearbeiten von verteilten Repositories

Bearbeiten Sie nach Bedarf die Konfigurations-, Authentifizierungs- und Paketauswahloptionen eines verteilten Repositorys.

Vorgehensweise

Definitionen zu Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

1. Klicken Sie auf **Menü** | **Software** | **Verteilte Repositories** und anschließend auf das gewünschte Repository.

   Der **Generator für verteilte Repositories** wird mit den Details zum verteilten Repository geöffnet.

2. Ändern Sie die Konfigurations-, Authentifizierungs- und Paketauswahloptionen nach Bedarf.

3. Klicken Sie auf **Speichern**.

Löschen von verteilten Repositories

Sie können verteilte Repositories aus HTTP- und FTP-Servern oder UNC-Freigaben löschen. Bei diesem Vorgang werden auch die in den Repositories gespeicherten Inhalte gelöscht.

Vorgehensweise

Definitionen zu Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

1 Klicken Sie auf **Menü | Software | Verteilte Repositories**, und klicken Sie dann neben dem gewünschten Repository auf **Löschen**.

2 Klicken Sie im Dialogfeld **Repository löschen** auf **OK**.



Beim Löschen des Repositorys werden die Pakete, die sich auf dem System mit dem Repository befinden, nicht gelöscht.

Gelöschte Repositories werden aus der Repository-Liste entfernt.

Verwenden von lokalen verteilten Repositories, die nicht verwaltet werden

Sie können Inhalte aus dem Master-Repository in ein verteiltes Repository kopieren, das nicht verwaltet wird.

Nachdem ein nicht verwaltet Repository erstellt wurde, müssen Sie verwaltete Systeme manuell so konfigurieren, dass sie Dateien aus dem nicht verwalteten Repository beziehen.

Definitionen zu Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

Vorgehensweise

1 Kopieren Sie alle Dateien und Unterverzeichnisse im Ordner des Master-Repositorys auf dem Server.

   Standardmäßig befindet sich dieser in folgendem Speicherort auf Ihrem Server: `C:\Programme\McAfee\ePO\4.6.0\DB\Software`

2 Fügen Sie die kopierten Dateien und Unterordner in den Repository-Ordner auf dem System des verteilten Repositorys ein.

3 Konfigurieren Sie eine Agenten-Richtlinie für verwaltete Systeme zum Verwenden des neuen, nicht verwalteten verteilten Repositorys:

   a Klicken Sie auf **Menü | Richtlinie | Richtlinienkatalog**, und wählen Sie dann in der Dropdown-Liste **Produkt** den Eintrag **McAfee Agent** und in der Dropdown-Liste **Kategorie** den Eintrag **Repository** aus.

   b Klicken Sie auf eine vorhandene Agenten-Richtlinie, oder erstellen Sie eine neue.

   Auf den Registerkarten mit den Optionen für eine Richtlinie können Sie nicht festlegen, dass die Richtlinienvererbung unterbrochen werden soll. Daher müssen Sie sich beim Anwenden dieser Richtlinie vergewissern, dass nur die gewünschten Systeme die Richtlinie zum Verwenden des nicht verwalteten verteilten Repositorys erhalten und erben.

   c Klicken Sie auf der Registerkarte **Repositories** auf **Hinzufügen**.

   Das Fenster **Repository hinzufügen** wird angezeigt.

   d Geben Sie einen Namen in das Textfeld **Repository-Name** ein.

   Bei dem Namen muss es sich nicht um den Namen des Systems handeln, das als Host für das Repository dient.

   e Wählen Sie unter **Dateien abrufen von** den Typ des Repositorys aus.

f Geben Sie unter **Konfiguration** den Speicherort des Repositorys mithilfe der entsprechenden Syntax für den Repository-Typ ein.

g Geben Sie eine Portnummer ein, oder behalten Sie den Standardport bei.

h Konfigurieren Sie die Anmeldeinformationen zur Authentifizierung nach Bedarf.

i Klicken Sie auf **OK**, um das neue verteilte Repository zur Liste hinzuzufügen.

j Wählen Sie das neue Repository in der Liste aus.

   Der Typ **Lokal** gibt an, dass es nicht von ePolicy Orchestrator verwaltet wird. Wenn in der **Repository-Liste** ein nicht verwaltetes Repository ausgewählt wird, sind die Schaltflächen **Bearbeiten** und **Löschen** aktiviert.

k Klicken Sie auf **Speichern**.

Jedes System, auf das diese Richtlinie angewendet wird, empfängt die neue Richtlinie bei der nächsten Agent-zu-Server-Kommunikation.

Arbeiten mit den Repository-Listen-Dateien

Sie können die Repository-Listen-Dateien SITELIST.XML und SITEMGR.XML exportieren.

Diese Dateien werden folgendermaßen verwendet:

- SITELIST.XML – Wird vom Agenten und unterstützten Produkten verwendet.
- SITEMGR.XML – Wird bei einer erneuten Installation des McAfee ePO-Servers oder beim Import in andere McAfee ePO-Server verwendet, die mit denselben verteilten Repositories oder Quellsites arbeiten.

Exportieren der Repository-Listen-Datei SITELIST.XML

Sie können die Repository-Listen-Datei (`SITELIST.XML`) für die manuelle Ausbringung auf Systemen oder für den Import während der Installation von unterstützten Produkten exportieren.

Vorgehensweise

Definitionen zu Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

1. Klicken Sie auf **Menü** | **Software** | **Master-Repository**, und klicken Sie dann auf **Aktionen** | **Sitelist exportieren**.

   Das Dialogfeld **Dateidownload** wird angezeigt.

2. Klicken Sie auf **Speichern**, wechseln Sie zu dem Speicherort, in dem die Datei `SITELIST.XML` gespeichert werden soll, und klicken Sie dann auf **Speichern**.

Sobald Sie diese Datei exportiert haben, können Sie sie während der Installation von unterstützten Produkten importieren. Anweisungen hierzu finden Sie im *Installationshandbuch* für das entsprechende Produkt.

Sie können die Repository-Liste auch auf verwaltete Systeme verteilen und sie anschließend auf den Agenten anwenden.

Exportieren der Repository-Liste zur Sicherung oder für die Verwendung auf anderen Servern

Mithilfe der exportierten Datei SITEMGR.XML können Sie verteilte Repositories und Quellsites wiederherstellen, wenn Sie den McAfee ePO-Server erneut installieren oder wenn Sie verteilte Repositories oder Quellsites auf einem anderen McAfee ePO-Server freigeben möchten.

Sie können diese Datei auf den Seiten **Verteilte Repositories** oder **Quellsites** exportieren. Wenn Sie jedoch diese Datei auf einer der beiden Seiten importieren, werden nur diejenigen Elemente aus der Datei importiert, die auf dieser Seite aufgeführt sind. Wenn zum Beispiel diese Datei auf der Seite **Verteilte Repositories** importiert wird, werden nur die verteilten Repositories in der Datei importiert. Wenn Sie also sowohl die verteilten Repositories als auch die Quellsites importieren möchten, müssen Sie die Datei jeweils von der entsprechenden Seite importieren.

Definitionen zu Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

Vorgehensweise

1. Klicken Sie auf **Menü** | **Software** | **Verteilte Repositories** (oder **Quellsites**), klicken Sie dann auf **Aktionen** | **Repositories exportieren** (oder **Quellsites exportieren**).

   Das Dialogfeld **Dateidownload** wird angezeigt.

2. Klicken Sie auf **Speichern**, wechseln Sie zu dem Speicherort, in dem die Datei gespeichert werden soll, und klicken Sie dann auf **Speichern**.

Importieren verteilter Repositories aus der Repository-Liste

Einen Import verteilter Repositories aus der Datei SITEMGR.XML führen Sie durch, nachdem Sie einen Server neu installiert haben oder wenn Sie möchten, dass ein Server die gleichen verteilten Repositories wie ein anderer Server verwenden soll.

Vorgehensweise

Definitionen zu Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

1. Klicken Sie auf **Menü** | **Software** | **Verteilte Repositories** und anschließend auf **Aktionen** | **Repositories importieren**.

   Die Seite **Repositories importieren** wird angezeigt.

2. Wechseln Sie zur exportierten Datei `SITEMGR.XML`, wählen Sie sie aus, und klicken Sie auf **OK**. Das verteilte Repository wird in den Server importiert.

3. Klicken Sie auf **OK**.

Die ausgewählten Repositories werden zur Liste der Repositories auf diesem Server hinzugefügt.

Importieren von Quellsites aus der Datei SITEMGR.XML

Einen Import von Quellsites aus einer Repository-Listen-Datei führen Sie durch, nachdem Sie einen Server neu installiert haben oder wenn Sie möchten, dass zwei Server die gleichen verteilten Repositories verwenden sollen.

Vorgehensweise

Definitionen zu Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

1. Klicken Sie auf **Menü** | **Konfiguration** | **Server-Einstellungen**, wählen Sie in der Liste **Einstellungskategorien** den Eintrag **Quellsites** aus, und klicken Sie dann auf **Bearbeiten**.

   Die Seite **Quellsites: Bearbeiten** wird angezeigt.

2. Klicken Sie auf **Importieren**. Die Seite **Repositories importieren** wird angezeigt.

3 Wechseln Sie zur exportierten Datei SITEMGR.XML, wählen Sie sie aus, und klicken Sie auf **OK**.

   Die Seite **Quellsites importieren** wird angezeigt.

4 Wählen Sie die gewünschten Quellsites aus, die auf diesen Server importiert werden sollen, und klicken Sie auf **OK**.

Die ausgewählten Quellsites werden zur Liste der Repositories auf diesem Server hinzugefügt.

Ändern von Anmeldeinformationen für mehrere verteilte Repositories

Ändern Sie die Anmeldeinformationen für mehrere verteilte Repositories des gleichen Typs. Dies ist in Umgebungen mit zahlreichen verteilten Repositories hilfreich.

Vorgehensweise

Definitionen zu Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

1. Klicken Sie auf **Menü | Verteilte Repositories**.

   Die Seite **Verteilte Repositories** wird angezeigt.

2. Klicken Sie auf **Aktionen**, und wählen Sie **Anmeldeinformationen ändern** aus.

   Die Seite **Repository-Typ** des Assistenten **Anmeldeinformationen ändern** wird angezeigt.

3. Wählen Sie den Typ des verteilten Repositorys aus, für das Sie Anmeldeinformationen ändern möchten, und klicken Sie dann auf **Weiter**.

   Die Seite **Repository-Auswahl** wird angezeigt.

4. Wählen Sie die gewünschten verteilten Repositories aus, und klicken Sie anschließend auf **Weiter**.

   Die Seite **Anmeldeinformationen** wird angezeigt.

5. Bearbeiten Sie die Anmeldeinformationen nach Bedarf, und klicken Sie dann auf **Weiter**.

   Daraufhin wird die Seite **Zusammenfassung** angezeigt.

6. Überprüfen Sie die Informationen, und klicken Sie dann auf **Speichern**.

7 Registrierte Server

Sie können auf zusätzliche Server zugreifen, indem Sie sie bei Ihrem McAfee ePO-Server registrieren. Mithilfe registrierter Server können Sie Ihre Software auf externen Servern integrieren. Beispielsweise können Sie einen LDAP-Server für die Verbindung mit Ihrem Active Directory-Server registrieren.

McAfee ePolicy Orchestrator kann mit folgenden Servern kommunizieren:

- Anderen McAfee ePO-Servern
- Zusätzlichen Remote-Datenbank-Servern
- LDAP-Servern
- HTTP-Servern
- Ticket-Servern

Jeder dieser Typen von registrierten Servern unterstützt oder ergänzt die Funktion von ePolicy Orchestrator und anderen Erweiterungen und Produkten von McAfee und Drittanbietern.

Inhalt

Registrieren von McAfee ePO-Servern

Sie können zusätzliche McAfee ePO-Server zum Gebrauch mit Ihrem McAfee ePO-Haupt-Server registrieren, um Daten zu sammeln oder zu aggregieren.

Vorgehensweise

Definitionen zu Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

1. Wählen Sie **Menü** | **Konfiguration** | **Registrierte Server** aus, und klicken Sie dann auf **Neuer Server**.
2. Wählen Sie auf der Seite **Beschreibung** im Menü **Server-Typ** die Option **ePO** aus, geben Sie einen eindeutigen Namen sowie Anmerkungen an, und klicken Sie dann auf **Weiter**.
3. Geben Sie zum Konfigurieren des Servers die folgenden Informationen an:

Option	Definition
Authentifizierungstyp	Gibt an, welcher Typ von Authentifizierung für diese Datenbank verwendet werden soll. Dazu gehören: • **Windows-Authentifizierung** • **SQL-Authentifizierung**
Client-Task-Freigabe	Gibt an, ob der Client-Task für diesen Server aktiviert oder deaktiviert sein soll.
Datenbankname	Geben Sie den Namen für diese Datenbank an.
Datenbankport	Geben Sie den Port für diese Datenbank an.
Datenbank-Server	Geben Sie den Namen der Datenbank für diesen Server an. Sie können eine Datenbank mithilfe des DNS-Namens oder der IP-Adresse (IPv4 oder IPv6) angeben.
ePO-Version	Gibt die Version des McAfee ePO-Servers an, der registriert werden soll.
Kennwort	Geben Sie das Kennwort für diesen Server an.
Richtlinienfreigabe	Gibt an, ob die Richtlinienfreigabe für diesen Server aktiviert oder deaktiviert sein soll.
SQL-Server-Instanz	Hier können Sie festlegen, ob es sich um den standardmäßigen Server oder eine bestimmte Instanz handelt. Geben Sie für eine bestimmte Instanz den Instanznamen an. Bevor Sie eine Verbindung zu einer bestimmten SQL-Instanz mit deren Instanznamen herstellen, müssen Sie sicherstellen, dass der SQL Browser-Dienst ausgeführt wird. Wenn der SQL Browser-Dienst nicht ausgeführt wird, geben Sie die Portnummer an. Wählen Sie die standardmäßige SQL-Server-Instanz aus, und geben Sie die Portnummer ein, um eine Verbindung zu der SQL-Server-Instanz herzustellen.
SSL-Kommunikation mit Datenbank-Server	Geben Sie an, ob ePolicy Orchestrator per SSL (Secure Socket Layer) mit diesem Datenbank-Server kommuniziert. Die folgenden Optionen sind möglich: • **SSL verwenden (wenn möglich)** • **Immer SSL verwenden** • **Niemals SSL verwenden**
Verbindung testen	Überprüft die Verbindung für den beschriebenen Server.
Systeme übertragen	Gibt an, ob die Fähigkeit zum Übertragen von Systemen bei diesem Server aktiviert oder deaktiviert ist. Wenn diese Option aktiviert ist, wählen Sie aus, ob **Automatischer Sitelist-Import** oder **Manueller Sitelist-Import** verwendet werden soll. Bei Auswahl von **Manueller Sitelist-Import** ist es möglich, dass ältere Versionen von McAfee Agent (Version 4.0 und früher) keinen Kontakt mehr mit der Agentensteuerung aufnehmen können. Dies kann der Fall sein, wenn: • Systeme von diesem McAfee ePO-Server auf den registrierten McAfee ePO-Server übertragen werden. • der Name einer Agentensteuerung alphanumerisch vor dem McAfee ePO-Server-Namen in der angegebenen Sitelist angezeigt wird. • die älteren Agenten diese Agentensteuerung verwenden.

Option	Definition
NTLMv2 verwenden	Sie können optional auswählen, dass das NT-LAN-Manager-Authentifizierungsprotokoll verwendet werden soll. Wählen Sie diese Option aus, wenn der Server, den Sie registrieren möchten, dieses Protokoll nutzt.
Benutzername	Geben Sie den Benutzernamen für diesen Server an.

4 Klicken Sie auf **Speichern**.

Registrieren von LDAP-Servern

Sie benötigen einen registrierten LDAP-Server (Lightweight Directory Access Protocol), um Richtlinienzuweisungsregeln verwenden sowie dynamisch zugewiesene Berechtigungssätze und die Active Directory-Benutzeranmeldung aktivieren zu können.

Vorgehensweise

Definitionen zu Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

1 Wählen Sie **Menü** | **Konfiguration** | **Registrierte Server** aus, und klicken Sie dann auf **Neuer Server**.

2 Wählen Sie auf der Seite **Beschreibung** im Menü **Server-Typ** die Option **LDAP-Server** aus, geben Sie einen eindeutigen Namen und eine Beschreibung an, und klicken Sie dann auf **Weiter**.

3 Wählen Sie in der Liste **LDAP-Server-Typ** aus, ob Sie einen OpenLDAP- oder einen Active Directory-Server registrieren möchten.



Bei den nachfolgenden Anweisungen wird davon ausgegangen, dass ein Active Directory-Server konfiguriert werden soll. Wo erforderlich, sind entsprechende Informationen für OpenLDAP-Server aufgeführt.

4 Wählen Sie im Abschnitt **Server-Name** aus, ob Sie einen Domänennamen oder einen bestimmten Server-Namen angeben möchten.

Verwenden Sie Domänennamen im DNS-Format (z. B. interneDomäne.com) und vollqualifizierte Domänennamen oder IP-Adressen für Server (z. B. server1.interneDomäne.com oder 192.168.75.101).

Bei Verwendung von Domänennamen haben Sie Failover-Unterstützung und erhalten die Möglichkeit, nur Server von einer bestimmten Site auszuwählen (wenn gewünscht).



Bei OpenLDAP-Servern können nur Server-Namen verwendet werden. Sie können nicht nach der Domäne angegeben werden.

5 Wählen Sie aus, ob Sie den **Globalen Katalog verwenden** möchten.

Diese Option ist standardmäßig deaktiviert. Eine Aktivierung kann zu deutlichen Verbesserungen bei der Leistung führen. Diese Option sollte jedoch nur dann aktiviert werden, wenn es sich bei der registrierten Domäne um die übergeordnete Domäne von nur lokalen Domänen handelt. Wenn sie auch nicht-lokale Domänen enthält, kann beim Verfolgen von Weiterleitungen beträchtlicher nicht-lokaler Netzwerkverkehr anfallen, was sich möglicherweise negativ auf die Leistung auswirkt.



Die Option **Globalen Katalog verwenden** steht bei OpenLDAP-Servern nicht zur Verfügung.

6 Wenn Sie diese Option **Globalen Katalog verwenden** deaktiviert haben, wählen Sie aus, ob Sie **Weiterleitung suchen** aktivieren möchten.

   Das Suchen von Weiterleitungen kann sich negativ auf die Leistung auswirken, wenn durch diese Funktion nicht-lokaler Netzwerkverkehr verursacht wird (wobei es keine Rolle spielt, ob ein globaler Katalog verwendet wird oder nicht).

7 Legen Sie mithilfe der Option **SSL verwenden** fest, ob mit diesem Server über SSL kommuniziert werden soll.

8 Wenn Sie einen OpenLDAP-Server konfigurieren, geben Sie den **Port** ein.

9 Geben Sie **Benutzername** und **Kennwort** ein.

   Das sollten die Anmeldeinformationen für ein Administratorkonto auf dem Server sein. Verwenden Sie für Active Directory-Server das Format `Domäne\Benutzername`, und für OpenLDAP-Server das Format `cn=Benutzer,dc=Domäne,dc=com`.

10 Geben Sie entweder einen **Site-Namen** für den Server ein, oder wählen Sie einen Namen aus, indem Sie auf **Durchsuchen** klicken und zu der Site wechseln.

11 Klicken Sie auf **Verbindung testen**, um zu überprüfen, ob die Kommunikation mit dem Server wie angegeben funktioniert. Falls erforderlich, ändern Sie die Informationen.

12 Klicken Sie auf **Speichern**, um den Server zu registrieren.

Registrieren von SNMP-Servern

Zum Empfangen eines SNMP-Traps müssen Sie die SNMP-Server-Informationen hinzufügen, damit ePolicy Orchestrator weiß, wohin der Trap gesendet werden soll.

Definitionen zu Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

Vorgehensweise

1 Klicken Sie auf **Menü** | **Konfiguration** | **Registrierte Server**, und klicken Sie dann auf **Neuer Server**.

2 Wählen Sie auf der Seite **Beschreibung** als Server-Typ **SNMP-Server** aus, geben Sie den Namen und mögliche weitere Informationen zu dem Server an, und klicken Sie dann auf **Weiter**.

3 Wählen Sie in der Dropdown-Liste **Adresse** einen der folgenden Typen für Server-Adressen aus, und geben Sie dann die Adresse ein:

   Tabelle 7-1 Optionsdefinitionen

Option	Definition
DNS-Name	Gibt den DNS-Namen des registrierten Servers an.
IPv4	Gibt die IPv4-Adresse des registrierten Servers an.
IPv6	Gibt den DNS-Namen des registrierten Servers an, der eine IPv6-Adresse hat.

4 Wählen Sie die von Ihrem Server verwendete SNMP-Version aus:

   - Wenn Sie als SNMP-Server-Version **SNMPv1** oder **SNMPv2c** auswählen, geben Sie unter **Sicherheit** die Community-Zeichenfolge des Servers ein.
   - Wenn Sie **SNMPv3** auswählen, geben Sie die Details für die **SNMPv3-Sicherheit** an.

5 Klicken Sie auf **Test-Trap senden**, um Ihre Konfiguration zu testen.

6 Klicken Sie auf **Speichern**.

Der hinzugefügte SNMP-Server wird auf der Seite **Registrierte Server** angezeigt.

Registrieren eines Datenbank-Servers

Bevor Sie Daten von einem Datenbank-Server abrufen können, müssen Sie diesen bei ePolicy Orchestrator registrieren.

Vorgehensweise

Definitionen zu Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

1. Öffnen Sie die Seite **Registrierte Server**. Wählen Sie **Menü** | **Konfiguration** | **Registrierte Server** aus, und klicken Sie dann auf **Neuer Server**.
2. Wählen Sie in der Dropdown-Liste **Server-Typ** den Eintrag **Datenbank-Server** aus, geben Sie einen Server-Namen und optional eine Beschreibung ein, und klicken Sie dann auf **Weiter**.
3. Wählen Sie in der Dropdown-Liste der registrierten Typen einen **Datenbanktyp** aus. Geben Sie an, ob dieser Datenbanktyp als Standardeinstellung dienen soll.

   Wenn diesem Datenbanktyp bereits eine Standarddatenbank zugewiesen wurde, ist diese in der Zeile **Aktuelle Standarddatenbank für Datenbanktyp** angegeben.
4. Geben Sie den **Datenbankhersteller** an. Derzeit werden nur Microsoft SQL Server und MySQL unterstützt.
5. Geben Sie die Verbindungs- und Anmeldeinformationen für den Datenbank-Server ein.
6. Wenn Sie überprüfen möchten, ob alle Verbindungs- und Anmeldeinformationen korrekt eingegeben sind, klicken Sie auf **Verbindung testen**.

   Eine Statusmeldung zeigt an, ob der Vorgang erfolgreich war oder nicht.
7. Klicken Sie auf **Speichern**.

Freigeben von Objekten zwischen Servern

Oftmals lässt sich eine bestimmte Verhaltensweise eines ePolicy Orchestrator-Servers am einfachsten auf einem anderen Server replizieren, indem das Element, das dieses Verhalten beschreibt, exportiert und auf dem anderen Server importiert wird.

Exportieren von Objekten aus ePolicy Orchestrator

Oftmals lässt sich eine bestimmte Verhaltensweise eines ePolicy Orchestrator-Servers am einfachsten auf einem anderen Server replizieren, indem das Element, das dieses Verhalten beschreibt, exportiert und auf dem anderen Server importiert wird.

Aus ePolicy Orchestrator exportierte Elemente werden in XML-Dateien gespeichert, die die exportierten Elemente detailliert beschreiben. Aus einem McAfee ePO-Server exportierte Objekte werden im Browser in XML-Form angezeigt. Wie die XML-Datei angezeigt und gespeichert wird, hängt von Ihren Browser-Einstellungen ab.

Inhalte exportierter Dateien

Wenn mehrere Elemente exportiert wurden, enthält eine exportierte Datei meist ein äußeres enthaltendes Element mit dem Namen `<list>`. Wenn nur ein einzelnes Objekt exportiert wurde, kann dieses äußere enthaltende Element nach dem Objekt benannt sein (z. B. `<query>`). Alle ausführlicheren Inhalte hängen vom jeweiligen Typ des exportierten Elements ab.

Exportierbare Elemente

Die folgenden Elemente können exportiert werden. Installierte Erweiterungen können weitere Elemente zu dieser Liste hinzufügen. Ausführlichere Informationen dazu finden Sie in der Dokumentation der jeweiligen Erweiterung.

- Dashboards
- Berechtigungssätze
- Abfragen
- Berichte
- Server-Tasks
- Benutzer
- Automatische Antworten

Der aktuelle Inhalt der folgenden Elemente kann in Tabellenform exportiert werden.

- Audit-Protokoll
- Probleme

Importieren von Elementen in ePolicy Orchestrator

Aus einem ePolicy Orchestrator-Server exportierte Elemente können in einen anderen Server importiert werden.

ePolicy Orchestrator exportiert Elemente in XML-Dateien. Diese XML-Dateien enthalten genaue Beschreibungen der exportierten Elemente.

Importieren von Elementen

Beim Importieren von Elementen in ePolicy Orchestrator müssen bestimmte Regeln beachtet werden:

- Bis auf Benutzer werden alle Elemente standardmäßig mit privater Sichtbarkeit importiert. Andere Berechtigungen können Sie während oder nach dem Import anwenden.
- Wenn ein Element mit dem gleichen Namen bereits vorhanden ist, wird dem Namen des importierten Elements die Zeichenfolge "`(importiert)`" oder "`(Kopie)`" angefügt.
- Importierte Elemente, die eine Erweiterung oder ein Produkt benötigen, die bzw. das auf dem neuen Server nicht vorhanden ist, werden als ungültig gekennzeichnet.

In ePolicy Orchestrator können nur von ePolicy Orchestrator exportierte XML-Dateien importiert werden.

Genauere Angaben dazu, wie die verschiedenen Arten von Elementen importiert werden, finden Sie in den Dokumentationen zu den einzelnen Elementen.

Vergleich der Export- und Importfunktionalität in McAfee ePO-Servern der verschiedenen Versionen

Wenn Sie Daten von einem ePolicy Orchestrator-Server auf einen anderen verschieben möchten, ist dies bei einigen Datenobjekten problemlos möglich, während es bei anderen einige Einschränkungen zu beachten gilt.

Die Einschränkungen bei Export- und Importvorgängen hängen von der ePolicy Orchestrator-Version ab. Außerdem spielt es eine Rolle, ob die Daten wieder zurück auf den gleichen McAfee ePO-Server oder auf einen anderen Server importiert werden sollen. In den folgenden Tabellen sind die Funktionen und Einschränkungen beim Export und Import von Daten aufgelistet.

Tabelle 7-2 Vergleich der Exportfunktionalität in McAfee ePO-Servern der Version 4.5, 4.6 und 5.0

Datenobjekt	Verfügbar für Export aus McAfee ePO...		
	...Version 4.5	...Version 4.6	...Version 5.0
Agentensteuerungszuweisungen	Ja	Ja	Ja
Agentensteuerungseinstellungen Beinhaltet nicht "Agentensteuerungszuweisungen".	Nein	Nein	Nein
Automatische Antworten	Ja	Ja	Ja
Client-Task-Zuweisungen	Nein	Ja	Ja
Client-Task-Objekte	Nein	Ja	Ja
Kontakte	Nein	Nein	Nein
Dashboards	Nein	Ja	Ja
Als Ausnahmen gekennzeichnete entdeckte Systeme	Ja	Ja	Ja
Einstellungen für entdeckte Systeme Beinhaltet nicht "Als Ausnahmen gekennzeichnete entdeckte Systeme".	Nein	Nein	Nein
Verteilte Repositories	Ja	Ja	Ja
Protokollinformationen	Nein (außer bei Zusammenfassung)	Nein (außer bei Zusammenfassung)	Nein (außer bei Zusammenfassung)
Berechtigungssätze	Nein	Ja	Ja
Persönliche Einstellungen	Nein	Nein	Nein
Richtlinienzuweisungsregeln	Ja	Ja	Ja
Richtlinienzuweisungen	Nein	Ja	Ja
Richtlinienobjekte	Ja	Ja	Ja
Abfragen	Ja	Ja	Ja
Registrierte ausführbare Dateien	Nein	Nein	Nein
Registrierte Server	Nein	Nein	Nein
Berichte	Nicht zutreffend	Ja	Ja
Sicherheitsschlüssel	Ja	Ja	Ja

Tabelle 7-2 Vergleich der Exportfunktionalität in McAfee ePO-Servern der Version 4.5, 4.6 und 5.0 *(Fortsetzung)*

Datenobjekt	Verfügbar für Export aus McAfee ePO...		
	...Version 4.5	...Version 4.6	...Version 5.0
Server-Einstellungen Beinhaltet nicht "Sicherheitsschlüssel" und "Quellsites".	Nein	Nein	Nein
Server-Tasks	Nein	Ja	Ja
Quellsites	Ja	Ja	Ja
Systemstruktur	Ja	Ja	Ja
Tag-Katalog	Ja	Ja	Ja
Active Directory-Struktursynchronisierung	Nein	Nein	Nein
Struktursortierung	Nein	Nein	Nein
Benutzerkonfigurierte Optionen	Nein	Nein	Nein
Benutzer	Nein	Nein	Nein

Tabelle 7-3 Funktionalität bei Export aus einem McAfee ePO 4.5-Server auf einen anderen 5.0-Server

Datenobjekt	Kann exportiert werden...		Anmerkungen
	...aus McAfee ePO 4.5-Server	...auf anderen McAfee ePO 5.0-Server	
Agentensteuerungszuweisungen	Ja	Nein	Verwendung der ID führt dazu, dass strukturbasierte Zuweisungen ihren Speicherort verlieren. Informationen über ausgewählte Agentensteuerungen gehen verloren.
Agentensteuerungseinstellungen Beinhaltet nicht "Agentensteuerungszuweisungen".	Nein	Nicht zutreffend	
Automatische Antworten	Ja	Nein	Import wird abgelehnt.
Client-Task-Zuweisungen	Nein	Nicht zutreffend	
Client-Task-Objekte	Nein	Nicht zutreffend	
Kontakte	Nein	Nicht zutreffend	
Dashboards	Nein	Nicht zutreffend	
Als Ausnahmen gekennzeichnete entdeckte Systeme	Ja	Ja	
Einstellungen für entdeckte Systeme Beinhaltet nicht "Als Ausnahmen gekennzeichnete entdeckte Systeme".	Nein	Nicht zutreffend	

Tabelle 7-3 Funktionalität bei Export aus einem McAfee ePO 4.5-Server auf einen anderen 5.0-Server *(Fortsetzung)*

Datenobjekt	Kann exportiert werden...		Anmerkungen
	...aus McAfee ePO 4.5-Server	...auf anderen McAfee ePO 5.0-Server	
Verteilte Repositories	Ja	Ja (aber mit Einschränkungen)	Wenn die Repositories unterschiedliche Inhalte enthalten, kann die Ausschlussliste zu einer unvorhersehbaren Paketauswahl führen.
Protokollinformationen	Nein (außer bei Zusammenfassung)	Nein (außer bei Zusammenfassung)	
Berechtigungssätze	Nein	Nicht zutreffend	
Persönliche Einstellungen	Nein	Nicht zutreffend	
Richtlinienzuweisungsregeln	Ja	Nein	In den Export- und Importinformationen enthaltene eindeutige IDs werden abgelehnt.
Richtlinienzuweisungen	Nein	Nicht zutreffend	
Richtlinienobjekte	Ja	Nein	Die McAfee-Repository-Richtlinie enthält möglicherweise nicht die gleichen Einstellungen für McAfee ePO-Server und -Agentensteuerungen wie die alten Server, Agentensteuerungen sind möglicherweise nicht vorhanden und die Richtlinie kann fehlschlagen.
Abfragen	Ja (aber mit Einschränkungen)	Nein	Abfragen mit serverspezifischen Daten sind nach Import fehlerhaft (z. B. Tags, Gruppe, Richtlinie).
Registrierte ausführbare Dateien	Nein	Nicht zutreffend	
Registrierte Server	Nein	Nicht zutreffend	
Berichte	Nicht zutreffend	Nicht zutreffend	
Sicherheitsschlüssel	Ja	Ja	
Server-Einstellungen Beinhaltet nicht "Sicherheitsschlüssel" und "Quellsites".	Nein	Nicht zutreffend	
Server-Tasks	Nein	Nicht zutreffend	
Quellsites	Ja	Ja	
Systemstruktur	Ja (aber mit Einschränkungen)	Ja (aber mit Einschränkungen)	In der exportierten Datei muss vor dem Import in jeder Zeile die Zeichenfolge "Eigene Organisation\" entfernt werden.

Tabelle 7-3 Funktionalität bei Export aus einem McAfee ePO 4.5-Server auf einen anderen 5.0-Server *(Fortsetzung)*

Datenobjekt	Kann exportiert werden...		Anmerkungen
	...aus McAfee ePO 4.5-Server	...auf anderen McAfee ePO 5.0-Server	
Tag-Katalog	Ja	Nein	Serverspezifische Daten in bestimmten Tags führen dazu, dass diese Tags nach dem Import nicht verfügbar sind.
Active Directory-Struktursynchronisierung	Nein	Nicht zutreffend	
Struktursortierung	Nein	Nicht zutreffend	
Benutzerkonfigurierte Optionen	Nein	Nicht zutreffend	
Benutzer	Nein	Nicht zutreffend	

Tabelle 7-4 Funktionalität bei Export aus einem McAfee ePO 4.6-Server auf einen anderen 5.0-Server

Datenobjekt	Kann exportiert werden...		Anmerkungen
	...aus McAfee ePO 4.6-Server	...auf anderen McAfee ePO 5.0-Server	
Agentensteuerungszuweisungen	Ja	Nein	Verwendung der ID führt dazu, dass strukturbasierte Zuweisungen ihren Speicherort verlieren. Informationen über ausgewählte Agentensteuerungen gehen verloren.
Agentensteuerungseinstellungen Beinhaltet nicht "Agentensteuerungszuweisungen".	Nein	Nicht zutreffend	
Automatische Antworten	Ja	Nein	Import wird abgelehnt.
Client-Task-Zuweisungen	Nein	Nicht zutreffend	
Client-Task-Objekte	Nein	Nicht zutreffend	
Kontakte	Nein	Nicht zutreffend	
Dashboards	Nein	Nicht zutreffend	
Als Ausnahmen gekennzeichnete entdeckte Systeme	Ja	Ja	
Einstellungen für entdeckte Systeme Beinhaltet nicht "Als Ausnahmen gekennzeichnete entdeckte Systeme".	Nein	Nicht zutreffend	
Verteilte Repositories	Ja	Ja (aber mit Einschränkungen)	Wenn die Repositories unterschiedliche Inhalte enthalten, kann die Ausschlussliste zu einer unvorhersehbaren Paketauswahl führen.

Tabelle 7-4 Funktionalität bei Export aus einem McAfee ePO 4.6-Server auf einen anderen 5.0-Server *(Fortsetzung)*

Datenobjekt	Kann exportiert werden...		Anmerkungen
	...aus McAfee ePO 4.6-Server	...auf anderen McAfee ePO 5.0-Server	
Protokollinformationen	Nein (außer bei Zusammenfassung)	Nein (außer bei Zusammenfassung)	
Berechtigungssätze	Nein	Nicht zutreffend	
Persönliche Einstellungen	Nein	Nicht zutreffend	
Richtlinienzuweisungsregeln	Ja	Nein	In den Export- und Importinformationen enthaltene eindeutige IDs werden abgelehnt.
Richtlinienzuweisungen	Nein	Nicht zutreffend	
Richtlinienobjekte	Ja	Nein	Die McAfee-Repository-Richtlinie enthält möglicherweise nicht die gleichen Einstellungen für McAfee ePO-Server und -Agentensteuerungen wie die alten Server, Agentensteuerungen sind möglicherweise nicht vorhanden und die Richtlinie kann fehlschlagen.
Abfragen	Ja (aber mit Einschränkungen)	Nein	Abfragen mit serverspezifischen Daten sind nach Import fehlerhaft (z. B. Tags, Gruppe, Richtlinie).
Registrierte ausführbare Dateien	Nein	Nicht zutreffend	
Registrierte Server	Nein	Nicht zutreffend	
Berichte	Nicht zutreffend	Nicht zutreffend	
Sicherheitsschlüssel	Ja	Ja	
Server-Einstellungen Beinhaltet nicht "Sicherheitsschlüssel" und "Quellsites".	Nein	Nicht zutreffend	
Server-Tasks	Nein	Nicht zutreffend	
Quellsites	Ja	Ja	
Systemstruktur	Ja (aber mit Einschränkungen)	Ja (aber mit Einschränkungen)	In der exportierten Datei muss vor dem Import in jeder Zeile die Zeichenfolge "Eigene Organisation\" entfernt werden.
Tag-Katalog	Ja	Nein	Serverspezifische Daten in Tags führen dazu, dass diese Tags nach dem Import nicht verfügbar sind.
Active Directory-Struktursynchronisierung	Nein	Nicht zutreffend	

Tabelle 7-4 Funktionalität bei Export aus einem McAfee ePO 4.6-Server auf einen anderen 5.0-Server *(Fortsetzung)*

Datenobjekt	Kann exportiert werden...		Anmerkungen
	...aus McAfee ePO 4.6-Server	...auf anderen McAfee ePO 5.0-Server	
Struktursortierung	Nein	Nicht zutreffend	
Benutzerkonfigurierte Optionen	Nein	Nicht zutreffend	
Benutzer	Nein	Nicht zutreffend	

Tabelle 7-5 Funktionalität bei Export aus einem McAfee ePO 5.0-Server und Import in einen anderen 5.0-Server

Objekt	Kann exportiert werden...		Anmerkungen
	...aus McAfee ePO 5.0-Server	...auf anderen McAfee ePO 5.0-Server	
Agentensteuerungszuweisungen	Ja	Nein	Verwendung der ID führt dazu, dass strukturbasierte Zuweisungen ihren Speicherort verlieren. Informationen über ausgewählte Agentensteuerungen gehen verloren.
Agentensteuerungseinstellungen Beinhaltet nicht "Agentensteuerungszuweisungen".	Nein	Nicht zutreffend	
Automatische Antworten	Ja	Nein	Die Verwendung der ID für entsprechende Systemstrukturknoten führt zu einer falschen Filterkonfiguration oder einem Fehler.
Client-Task-Zuweisungen	Ja	Ja (aber mit Einschränkungen)	Wenn Tasks vor oder nach einer unterbrochenen Vererbung importiert werden, gehen Tasks mit unterbrochener Vererbung verloren und Task-Zuweisungen werden doppelt erstellt.
Client-Task-Objekte	Ja	Ja (aber mit Einschränkungen)	Der Inhalt des Master-Repositorys muss mit dem ursprünglichen Server übereinstimmen (gleiche Versionen), andernfalls sind Auswahlmöglichkeiten leer oder nicht vorhanden.
Kontakte	Nein	Nicht zutreffend	
Dashboards	Ja	Nein	Abfragen mit serverspezifischen Daten sind nach Import fehlerhaft (z. B. Tags, Gruppe, Richtlinie).
Als Ausnahmen gekennzeichnete entdeckte Systeme	Ja	Ja (aber mit Einschränkungen)	Ausnahmenkategorien werden nicht exportiert.

Tabelle 7-5 Funktionalität bei Export aus einem McAfee ePO 5.0-Server und Import in einen anderen 5.0-Server *(Fortsetzung)*

Objekt	Kann exportiert werden...		Anmerkungen
	...aus McAfee ePO 5.0-Server	...auf anderen McAfee ePO 5.0-Server	
Einstellungen für entdeckte Systeme Beinhaltet nicht "Als Ausnahmen gekennzeichnete entdeckte Systeme".	Nein	Nicht zutreffend	
Verteilte Repositories	Ja	Nein	Die Paket-Ausschlussliste ist nach dem Import nicht mehr vorhanden.
Protokollinformationen	Nein (außer bei Zusammenfassung)	Nein (außer bei Zusammenfassung)	
Berechtigungssätze	Ja	Ja (aber mit Einschränkungen)	Berechtigungssätze müssen die gleiche Systemstruktur und die gleichen Repository-Inhalte haben.
Persönliche Einstellungen	Nein	Nicht zutreffend	
Richtlinienzuweisungsregeln	Ja	Nein	IDs führen dazu, dass Server falsche Tags und registrierte Server verwenden.
Richtlinienzuweisungen	Ja	Nein	Mehrere Zuweisungen von Richtlinien für mehrere Richtlinienplätze bei einem Knoten werden nicht korrekt importiert.
Richtlinienobjekte	Ja	Nein	Die McAfee-Repository-Richtlinie enthält möglicherweise nicht die gleichen Einstellungen für McAfee ePO-Server und -Agentensteuerungen wie die alten Server, Agentensteuerungen sind möglicherweise nicht vorhanden und die Richtlinie kann fehlschlagen.
Abfragen	Ja (aber mit Einschränkungen)	Nein	Abfragen mit serverspezifischen Daten sind nach Import fehlerhaft (z. B. Tags, Gruppe oder Richtlinie).
Registrierte ausführbare Dateien	Nein	Nicht zutreffend	
Registrierte Server	Nein	Nicht zutreffend	
Berichte	Ja	Nein	Abfragen mit serverspezifischen Daten sind nach dem Import fehlerhaft (z. B. Tags, Gruppe oder Richtlinie).
Sicherheitsschlüssel	Ja	Ja	

Tabelle 7-5 Funktionalität bei Export aus einem McAfee ePO 5.0-Server und Import in einen anderen 5.0-Server *(Fortsetzung)*

Objekt	Kann exportiert werden...		Anmerkungen
	...aus McAfee ePO 5.0-Server	...auf anderen McAfee ePO 5.0-Server	
Server-Einstellungen Beinhaltet nicht "Sicherheitsschlüssel" und "Quellsites".	Nein	Nicht zutreffend	
Server-Tasks	Ja	Ja (aber mit Einschränkungen)	
Quellsites	Ja	Ja	
Systemstruktur	Ja	Ja	
Tag-Katalog	Ja	Nein	Serverspezifische Daten in Tags führen dazu, dass die Tags nach dem Import nicht verfügbar sind.
Active Directory-Struktursynchronisierung	Nein	Nicht zutreffend	
Struktursortierung	Nein	Nicht zutreffend	
Benutzerkonfigurierte Optionen	Nein	Nicht zutreffend	
Benutzer	Nein	Nicht zutreffend	

Tabelle 7-6 Export- und Importfunktionalität von McAfee ePO 5.0-Server-Tasks

Server-Task-Objekt	Auf anderen Server exportierbar?	Anmerkungen
Tasks, die Abfragen enthalten	Ja (aber mit Einschränkungen)	Bei von mehreren Tasks verwendeten Abfragen werden doppelte Tasks erstellt, wenn die Tasks zu unterschiedlichen Zeitpunkten importiert werden.
Tasks, die Dateipfade enthalten	Ja (aber mit Einschränkungen)	Dateipfade müssen auf Servern übereinstimmen, andernfalls werden einige Dateien möglicherweise nicht geschrieben (Wenn zum Beispiel der importierte Server kein Laufwerk "D:\" besitzt, können Dateien, die auf dem exportierten Server auf Laufwerk "D:\" gespeichert sind, beim Import nicht geschrieben werden.).
Systemsuche	Nein	Die für Gruppen und Tags verwendeten IDs führen zu einer fehlerhaften Übereinstimmung.
Tag-Kriterien ausführen	Nein	Die für Tags verwendeten IDs führen zu einer fehlerhaften Übereinstimmung.
Bericht ausführen	Nein	Die für Abfragen verwendeten IDs können zu einer fehlerhaften Übereinstimmung führen; Abfragen können serverspezifische Informationen enthalten.
Abfrage ausführen – Agenten aktualisieren	Ja (aber mit Einschränkungen)	Die Abfragen müssen den gleichen Inhalt haben, sonst gehen Einstellungen beim Task verloren.

Tabelle 7-6 Export- und Importfunktionalität von McAfee ePO 5.0-Server-Tasks *(Fortsetzung)*

Server-Task-Objekt	Auf anderen Server exportierbar?	Anmerkungen
Abfrage ausführen – Client-Task jetzt ausführen	Nein	Die verwendeten IDs können zu einer fehlerhaften Übereinstimmung führen.
Abfrage ausführen – Systeme verschieben	Nein	Die verwendeten IDs können zu einer fehlerhaften Übereinstimmung führen.
Abfrage ausführen – Tag ausschließen	Nein	Die verwendeten IDs können zu einer fehlerhaften Übereinstimmung führen.
Abfrage ausführen – Als Ausnahmen gekennzeichnete entdeckte Systeme	Ja (aber mit Einschränkungen)	Die zur Kategorieauswahl verwendete ID kann zu einer fehlerhaften Übereinstimmung führen.
Abfrage ausführen – McAfee Agent ausbringen	Nein	Agentensteuerungs-spezifische Daten stehen auf dem importierenden Server möglicherweise nicht zur Verfügung; das Kennwort ist in der exportierten Datei nicht enthalten.
Abfrage ausführen – Tag löschen	Nein	Die verwendeten IDs können zu einer fehlerhaften Übereinstimmung führen.
Abfrage ausführen – Richtlinie zuweisen	Nein	Auch wenn die Richtlinie vom Task importiert wurde, können die verwendeten IDs zu einer fehlerhaften Übereinstimmung und einem Task-Fehler führen.
Abfrage ausführen – Tag anwenden	Nein	Die verwendeten IDs können zu einer fehlerhaften Übereinstimmung führen.
Abfrage ausführen – Zur Systemstruktur hinzufügen	Nein	Die verwendeten IDs können zu einer fehlerhaften Übereinstimmung führen.
Zusammenfassung	Nein	Wenn bei Auswahl einzelner registrierter Server IDs verwendet werden, kann dies zu einer fehlerhaften Übereinstimmung führen; das Filtern von Eigenschaften kann serverspezifisch sein (Angewendete Richtlinien).
Repository-Replizierung	Ja (aber mit Einschränkungen)	Die Repositories müssen den gleichen Inhalt haben, sonst gehen Einstellungen beim Task verloren.
Repository-Abruf	Nein	Die für die Quellsite verwendete ID kann ein Problem verursachen. Die Repositories müssen den gleichen Inhalt haben, sonst gehen Einstellungen beim Task verloren.
X bereinigen	Ja (aber mit Einschränkungen)	Bei Verwendung einer Abfrage zum Bereinigen kann die für die Abfrage verwendete ID zu einer fehlerhaften Übereinstimmung bei Servern führen.
Abfragen exportieren	Nein	Abfragen können serverspezifische Daten enthalten, wodurch die Abfragen nach dem Import fehlerhaft sind.
Zweig eines Pakets wechseln	Ja (aber mit Einschränkungen)	Die Pakete müssen den gleichen Inhalt haben, sonst gehen Einstellungen beim Task verloren.
Active Directory-Synchronisierung	Nein	Die für den Speicherort verwendete ID kann, selbst wenn die Verzeichnisstruktur importiert wird, zu einer fehlerhaften Übereinstimmung führen.

Exportieren von Objekten und Daten aus dem ePolicy Orchestrator-Server

Exportierte Objekte und Daten können verwendet werden, um wichtige Daten zu sichern und die ePolicy Orchestrator-Server in einer Umgebung wiederherzustellen oder zu konfigurieren.

Die meisten in einem Server verwendeten Daten und Objekte können exportiert oder heruntergeladen werden, um angezeigt, umgewandelt oder in andere Server oder Anwendungen importiert zu werden. In der folgenden Tabelle sind die verschiedenen Elemente und die daran ausführbaren Aktionen aufgeführt. Sie können in HTML- und PDF-Dateien exportieren, um die Daten anzuzeigen, oder in CSV- bzw. XML-Dateien, um die Daten in anderen Anwendungen zu verwenden und umzuwandeln.

Objekttyp	Kann exportiert werden	Kann importiert werden	Exportformat
Automatische Antworten	X	X	XML
Client-Task-Objekte	X	X	XML
Dashboards	X	X	XML
Als Ausnahmen gekennzeichnete entdeckte Systeme	X	X	TXT
Definitionen von Berechtigungssätzen	X	X	XML
Richtlinienobjekte	X	X	XML
Richtlinienzuweisungen	X	X	XML
Abfragedefinitionen	X	X	XML
Abfragedaten	X		Mehrere
Berichte	X	X	XML
Repositories	X	X	XML
Server-Tasks	X	X	XML
Sitelists	X	X	XML
Subnetze (in Form einer Liste)	X	X	TXT
Systeme (in Form einer Liste, aus der Systemstruktur)	X	X	TXT
Tabellen (in Form eines Berichts oder einer Liste)	X		Mehrere
Tags	X	X	XML

Vorgehensweise

1. Klicken Sie auf der Seite, auf der die Objekte oder Daten angezeigt werden, auf **Aktionen**, und wählen Sie die gewünschte Option aus. So wählen Sie zum Beispiel beim Exportieren einer Tabelle die Option **Tabelle exportieren** aus und klicken dann auf **Weiter**.
2. Beim Exportieren von Inhalten, die in mehreren Formaten heruntergeladen werden können (z. B. Abfragedaten), wird die Seite **Exportieren** mit Konfigurationsoptionen geöffnet. Geben Sie die gewünschten Einstellungen an, und klicken Sie auf **Exportieren**.
3. Beim Exportieren von Objekten oder Definitionen (z. B. Client-Task-Objekte oder Definitionen) wird eines der folgenden Fenster angezeigt:
   - Ein Browser-Dialogfeld wird geöffnet, in dem Sie die Datei **Öffnen** oder **Speichern** können.
   - Die Seite **Exportieren** wird mit einem Link zu der Datei geöffnet. Klicken Sie mit der linken Maustaste auf den Link, um die Datei im Browser anzuzeigen. Klicken Sie mit der rechten Maustaste auf den Link, um die Datei zu speichern.

8 Agentensteuerungen

Agentensteuerungen leiten die Kommunikation zwischen Agenten und dem McAfee ePO-Server weiter.

Auf jedem McAfee ePO-Server befindet sich eine Master-Agentensteuerung. Sie können zusätzliche Agentensteuerungen auf Systemen im Netzwerk installieren.

Das Einrichten weiterer Agentensteuerungen bietet die folgenden Vorteile.

- Bessere Verwaltung einer größeren Anzahl von Produkten und Systemen über einen einzigen logischen ePolicy Orchestrator-Server, vorausgesetzt, die CPU auf dem Datenbank-Server wird nicht überlastet
- Fehlertoleranz und Lastausgleich bei der Kommunikation mit vielen Agenten (einschließlich räumlich verteilter Agenten)

Inhalt

Funktionsweise von Agentensteuerungen

Agentensteuerungen verteilen den bei Agent-zu-Server-Kommunikationen anfallenden Netzwerkverkehr, indem sie dafür sorgen, dass sich verwaltete Systeme oder Gruppen von Systemen an eine bestimmte Agentensteuerung wenden. Nach der Zuweisung kommuniziert ein verwaltetes System anstatt mit dem McAfee ePO-Haupt-Server mit der ihm zugewiesenen Agentensteuerung.

Die Steuerung stellt wie der McAfee ePO-Server aktualisierte Sitelists, Richtlinien und Richtlinienzuweisungsregeln bereit. Sie führt außerdem eine Zwischenspeicherung der Inhalte des Master-Repositorys durch, sodass Produktaktualisierungspakete, DAT-Dateien und andere benötigte Informationen von Agenten abgerufen werden können.



Wenn ein Agent bei seiner Steuerung eincheckt und diese nicht über die benötigten Aktualisierungen verfügt, ruft sie sie aus dem zugewiesenen Repository ab und legt sie im Cache ab. Gleichzeitig leitet die Steuerung die Aktualisierung an den Agenten weiter.

In dem Diagramm **Systeme pro Agentensteuerung** werden alle installierten Agentensteuerungen sowie die Anzahl der von jeder Steuerung verwalteten Agenten angezeigt.

Deinstallierte Agentensteuerungen werden in diesem Diagramm nicht angezeigt. Wenn eine Agentensteuerung deinstalliert wurde, der von einer Agentensteuerungs-Zuweisungsregel exklusiv Agenten zugewiesen sind, wird sie im Diagramm als **Agentensteuerung deinstalliert** geführt und die Anzahl von Agenten angezeigt, die immer noch versuchen, eine Verbindung zu dieser Steuerung herzustellen.

Wenn die Agentensteuerungen nicht ordnungsgemäß installiert sind, wird die Meldung **Agentensteuerung deinstalliert** angezeigt, was bedeutet, dass die Steuerung mit einigen Agenten nicht kommunizieren kann. Klicken Sie auf die Liste, um die Agenten anzuzeigen, die nicht mit der Steuerung kommunizieren können.

Mehrere Agentensteuerungen

Ein Netzwerk kann auch über mehrere Agentensteuerungen verfügen. Angenommen Sie besitzen eine große Anzahl von verwalteten Systemen, die über mehrere geographische Standorte oder über Ländergrenzen hinweg verteilt sind. In solchen und ähnlichen Fällen können Sie eine Organisation zu Ihren verwalteten Systemen hinzufügen, indem Sie verschiedene Gruppen unterschiedlichen Steuerungen zuweisen.

Steuerungsgruppen und -priorität

Bei Verwendung mehrerer Agentensteuerungen in einem Netzwerk sollten Sie diese gruppieren und priorisieren, um Netzwerkverbindungen sicherzustellen.

Steuerungsgruppen

Bei mehreren Agentensteuerungen in einem Netzwerk können Sie Steuerungsgruppen erstellen. Außerdem können Sie den Steuerungen in einer Gruppe Prioritäten zuweisen. Anhand der Steuerungspriorität erkennen die Agenten, mit welcher Steuerung sie zuerst kommunizieren sollen. Wenn die Steuerung mit der höchsten Priorität nicht verfügbar ist, wechselt der Agent zur nächsten Steuerung in der Liste. Die Prioritätsinformationen sind in der Repository-Liste (SITELIST.XML) in jedem Agenten enthalten. Wenn Sie Steuerungszuweisungen ändern, wird diese Datei während der Agent-zu-Server-Kommunikation aktualisiert. Nach dem Empfang der Zuweisung wartet der Agent mit deren Implementierung bis zur nächsten regelmäßig geplanten Kommunikation. Wenn Sie den Agenten sofort aktualisieren möchten, können Sie eine sofortige Agenten-Reaktivierung ausführen.

Das Gruppieren von Steuerungen und Zuweisen von Prioritäten lässt sich gemäß den Anforderungen der jeweiligen Umgebung anpassen. Für das Gruppieren von Steuerungen gibt es zwei Szenarien:

- **Verwenden mehrerer Steuerungen für den Lastausgleich**

  Sie haben ein Netzwerk mit einer großen Anzahl von verwalteten Systemen, für die die aus der Agent-zu-Server-Kommunikation und der Erzwingung von Richtlinien resultierende Netzwerklast möglichst verteilt werden soll. Sie können die Steuerungsliste so konfigurieren, dass die Agenten die Steuerungen, mit denen sie kommunizieren, nach dem Zufallsprinzip auswählen.

- **Einrichten eines alternativen Plans zum Sicherstellen der Agent-zu-Server-Kommunikation**

  Sie haben Systeme, die über mehrere geographische Standorte verteilt sind. Indem Sie jeder über diese Standorte verteilten Steuerung eine Priorität zuweisen, können Sie angeben, mit welchen Steuerungen die Agenten in welcher Reihenfolge kommunizieren sollen. So kann sichergestellt werden, dass die verwalteten Systeme in einem Netzwerk auf dem aktuellen Stand bleiben, indem alternative Kommunikationsmöglichkeiten für Agenten erstellt werden (so wie mit alternativen Repositories sichergestellt wird, dass den Agenten immer neue Aktualisierungen zur Verfügung stehen). Wenn die Steuerung mit der höchsten Priorität nicht verfügbar ist, wechselt der Agent zur Steuerung mit der nächsthöheren Priorität.

Außer innerhalb einer Gruppe von Steuerungen können Sie Steuerungsprioritäten auch über mehrere Gruppen von Steuerungen hinweg zuweisen. Auf diese Weise wird Ihre Umgebung weiter abgesichert, und Sie erhöhen damit die Wahrscheinlichkeit, dass Ihre Agenten jederzeit die benötigten Informationen empfangen können.

Sitelist-Dateien

Mithilfe der Dateien SITELIST.XML und SITELIST.INFO entscheidet der Agent, mit welcher Steuerung er kommuniziert. Diese Dateien werden bei jeder Aktualisierung der Steuerungszuweisungen und -prioritäten auf dem verwalteten System aktualisiert. Nachdem die Dateien aktualisiert wurden, implementiert der Agent die neue Zuweisung oder Priorität bei der nächsten geplanten Agent-zu-Server-Kommunikation.

Verwalten von Agentensteuerungen

Sie können in Ihrem Netzwerk Agentensteuerungen einrichten und ihnen McAfee Agents zuweisen.

Aufgaben

- *Zuweisen von McAfee Agents zu Agentensteuerungen* auf Seite 99
  Sie können Agenten zu bestimmten Steuerungen zuweisen. Die Zuweisung von Systemen kann einzeln, nach der Gruppe oder nach dem Subnetz erfolgen.
- *Verwalten von Agentensteuerungszuweisungen* auf Seite 100
  Führen Sie die allgemeinen Verwaltungsausgaben für Agentensteuerungszuweisungen durch.
- *Erstellen von Agentensteuerungsgruppen* auf Seite 101
  Mithilfe von Steuerungsgruppen wird die Verwaltung mehrerer Steuerungen in einem Netzwerk vereinfacht. Außerdem können Steuerungsgruppen bei Ihrer Alternativstrategie eine Rolle spielen.
- *Verwalten von Agentensteuerungsgruppen* auf Seite 101
  Führen Sie die allgemeinen Verwaltungsausgaben für Agentensteuerungsgruppen durch.
- *Verschieben von Agenten zwischen Steuerungen* auf Seite 102
  Sie können Agenten zu bestimmten Steuerungen zuweisen. Die Zuweisung von Systemen kann mithilfe von Zuweisungsregeln oder der Zuweisungspriorität für Agentensteuerungen sowie individuell mithilfe der Systemstruktur erfolgen.

Zuweisen von McAfee Agents zu Agentensteuerungen

Sie können Agenten zu bestimmten Steuerungen zuweisen. Die Zuweisung von Systemen kann einzeln, nach der Gruppe oder nach dem Subnetz erfolgen.

Steuerungszuweisungen können angeben, ob eine einzelne Steuerung oder eine Liste von Steuerungen verwendet werden soll. Die von Ihnen angegebene Liste kann aus einzelnen Steuerungen oder Gruppen von Steuerungen bestehen.

Vorgehensweise

Definitionen zu Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

1. Klicken Sie auf **Menü** | **Konfiguration** | **Agentensteuerungen**, und klicken Sie dann auf **Aktionen** | **Neue Zuweisung**.
2. Geben Sie einen eindeutigen Namen für die Zuweisung an.
3. Geben Sie die Agenten für diese Zuweisung mithilfe der folgenden Optionen für **Agenten-Kriterien** an:
   - Wechseln Sie zu einem **Speicherort in der Systemstruktur**.
   - Geben Sie die IP-Adresse, den IP-Bereich oder die Subnetzmaske von verwalteten Systemen in das Feld **Agenten-Subnetz** ein.

4 Geben Sie die **Steuerungspriorität** mithilfe einer der beiden folgenden Optionen an:

- **Alle Agentensteuerungen verwenden** – Die Agenten wählen nach dem Zufallsprinzip aus, mit welcher Steuerung sie kommunizieren.
- **Liste benutzerdefinierter Steuerungen verwenden** – Wählen Sie bei Verwendung einer Liste benutzerdefinierter Steuerungen die Steuerung oder Steuerungsgruppe im Dropdown-Menü aus.



Bei Verwendung einer Liste benutzerdefinierter Steuerungen können Sie mit **+** und **-** weitere Agentensteuerungen hinzufügen bzw. entfernen (eine Agentensteuerung kann auch in mehreren Gruppen enthalten sein). Ändern Sie die Priorität von Steuerungen mittels Ziehen und Ablegen. Mit welcher Steuerung die Agenten die Kommunikation zuerst versuchen, richtet sich nach der Priorität.

Verwalten von Agentensteuerungszuweisungen

Führen Sie die allgemeinen Verwaltungsausgaben für Agentensteuerungszuweisungen durch.

Klicken Sie zum Durchführen dieser Aktionen auf **Menü** | **Konfiguration** | **Agentensteuerungen**, und klicken Sie dann in **Zuweisungsregeln für Steuerung** auf **Aktionen**.

Aktion	Vorgehensweise
Löschen einer Steuerungszuweisung	Klicken Sie in der Zeile mit der ausgewählten Zuweisung auf **Löschen**.
Bearbeiten einer Steuerungszuweisung	Klicken Sie für die ausgewählte Zuweisung auf **Bearbeiten**. Die Seite **Agentensteuerungszuweisung** wird geöffnet, auf der Sie Folgendes angeben können: • **Zuweisungsname** – Der eindeutige Name, mit dem diese Steuerungszuweisung identifiziert wird. • **Agenten-Kriterien** – Die Systeme, die in dieser Zuweisung enthalten sind. Sie können Systemstrukturgruppen hinzufügen und entfernen oder die Liste der Systeme im Textfeld ändern. • **Steuerungspriorität** – Wählen Sie aus, ob alle Agentensteuerungen oder eine Liste benutzerdefinierter Steuerungen verwendet werden soll. Wenn **Alle Agentensteuerungen verwenden** ausgewählt ist, wählen Agenten ihre Steuerung für die Kommunikation nach dem Zufallsprinzip aus. Mittels Ziehen und Ablegen können Sie die Priorität von Steuerungen in Ihrer Liste benutzerdefinierter Steuerungen schnell ändern.
Exportieren von Steuerungszuweisungen	Klicken Sie auf **Exportieren**. Die Seite **Agentensteuerungszuweisungen herunterladen** wird geöffnet, auf der Sie die Datei AGENTHANDLERASSIGNMENTS.XML anzeigen oder herunterladen können.
Importieren von Steuerungszuweisungen	Klicken Sie auf **Importieren**. Das Dialogfeld **Aktion: Importieren** wird geöffnet, in dem Sie zu einer zuvor heruntergeladenen Datei mit dem Namen AGENTHANDLERASSIGNMENTS.XML wechseln können.
Bearbeiten der Priorität von Steuerungszuweisungen	Klicken Sie auf **Priorität bearbeiten**. Die Seite **Agentensteuerungszuweisung | Priorität bearbeiten** wird geöffnet, auf der Sie die Priorität von Steuerungszuweisungen mittels Ziehen und Ablegen ändern.
Anzeigen einer Zusammenfassung der Details einer Steuerungszuweisung	Klicken Sie in der Zeile mit der ausgewählten Zuweisung auf **>**.

Erstellen von Agentensteuerungsgruppen

Mithilfe von Steuerungsgruppen wird die Verwaltung mehrerer Steuerungen in einem Netzwerk vereinfacht. Außerdem können Steuerungsgruppen bei Ihrer Alternativstrategie eine Rolle spielen.

Vorgehensweise

Definitionen zu Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

1. Klicken Sie auf **Menü** | **Konfiguration** | **Agentensteuerungen**, und klicken Sie dann unter **Steuerungsgruppen** auf **Neue Gruppe**.

   Die Seite **Gruppe hinzufügen/bearbeiten** wird angezeigt.

2. Geben Sie den Gruppennamen und die Details zu **Eingeschlossene Steuerungen** an. Dazu gehören:
   - Klicken Sie zum Verwenden eines Lastausgleichs von einem Drittanbieter auf **Lastausgleich verwenden**, und füllen Sie dann die Felder **Virtueller DNS-Name** und **Virtuelle IP-Adresse** aus (beide Felder sind erforderlich).
   - Klicken Sie auf **Liste benutzerdefinierter Steuerungen verwenden**, um die in dieser Gruppe enthaltenen Agentensteuerungen anzugeben.



Bei Verwendung einer Liste benutzerdefinierter Steuerungen wählen Sie die Steuerungen in der Dropdown-Liste **Eingeschlossene Steuerungen** aus. Mit **+** und - können Sie weitere Agentensteuerungen zur Liste hinzufügen bzw. aus ihr entfernen (eine Agentensteuerung kann auch in mehreren Gruppen enthalten sein). Ändern Sie die Priorität von Steuerungen mittels Ziehen und Ablegen. Mit welcher Steuerung die Agenten die Kommunikation zuerst versuchen, richtet sich nach der Priorität.

3. Klicken Sie auf **Speichern**.

Verwalten von Agentensteuerungsgruppen

Führen Sie die allgemeinen Verwaltungsausgaben für Agentensteuerungsgruppen durch.

Klicken Sie zum Durchführen dieser Aktionen auf **Menü** | **Konfiguration** | **Agentensteuerungen**, und klicken Sie dann auf den Monitor **Steuerungsgruppen**.

Aktion	Vorgehensweise
Löschen einer Steuerungsgruppe	Klicken Sie in der Zeile mit der ausgewählten Gruppe auf **Löschen**.
Bearbeiten einer Steuerungsgruppe	Klicken Sie auf eine Steuerungsgruppe. Die Seite **Gruppe hinzufügen/bearbeiten** wird geöffnet, auf der Sie Folgendes angeben können: • **Virtueller DNS-Name** – Der eindeutige Name, mit dem diese Steuerungsgruppe identifiziert wird. • **Virtuelle IP-Adresse** – Die mit dieser Gruppe verknüpfte IP-Adresse. • **Eingeschlossene Steuerungen** – Wählen Sie aus, ob ein Drittanbieter-Lastausgleich oder eine Liste benutzerdefinierter Steuerungen verwendet werden soll. Mithilfe einer Liste benutzerdefinierter Steuerungen geben Sie an, mit welchen Steuerungen (und in welcher Reihenfolge) Agenten kommunizieren, die dieser Gruppe zugewiesen sind.
Aktivieren oder Deaktivieren einer Steuerungsgruppe	Klicken Sie in der Zeile mit der ausgewählten Gruppe auf **Aktivieren** bzw. **Deaktivieren**.

Verschieben von Agenten zwischen Steuerungen

Sie können Agenten zu bestimmten Steuerungen zuweisen. Die Zuweisung von Systemen kann mithilfe von Zuweisungsregeln oder der Zuweisungspriorität für Agentensteuerungen sowie individuell mithilfe der Systemstruktur erfolgen.

Steuerungszuweisungen können angeben, ob eine einzelne Steuerung oder eine Liste von Steuerungen verwendet werden soll. Die von Ihnen angegebene Liste kann aus einzelnen Steuerungen oder Gruppen von Steuerungen bestehen.

Aufgaben

- *Gruppieren von Agenten mithilfe von Agentensteuerungszuweisungen* auf Seite 102
  Sie können Agentensteuerungszuweisungen erstellen, um McAfee Agents in Gruppen zusammenzufassen.
- *Gruppieren von Agenten nach Zuweisungspriorität* auf Seite 103
  Fassen Sie Agenten in Gruppen zusammen, und weisen Sie sie einer Agentensteuerung zu, die Zuweisungspriorität verwendet.
- *Gruppieren von Agenten mithilfe der Systemstruktur* auf Seite 104
  Gruppieren Sie Agenten, und weisen Sie ihnen mithilfe der Systemstruktur eine Agentensteuerung zu.

Gruppieren von Agenten mithilfe von Agentensteuerungszuweisungen

Sie können Agentensteuerungszuweisungen erstellen, um McAfee Agents in Gruppen zusammenzufassen.

Steuerungszuweisungen können angeben, ob eine einzelne Steuerung oder eine Liste von Steuerungen verwendet werden soll. Die von Ihnen angegebene Liste kann aus einzelnen Steuerungen oder Gruppen von Steuerungen bestehen.



Beim Zuweisen von Agenten zu Agentensteuerungen sollten Sie auf geographische Nähe achten, um unnötigen Netzwerkverkehr zu vermeiden.

Vorgehensweise

Definitionen zu Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

1. Klicken Sie auf **Menü** | **Konfiguration** | **Agentensteuerungen**, und klicken Sie dann auf die erforderliche Regel unter **Zuweisungsregeln für Steuerung**.

   Die Seite **Agentensteuerungszuweisung** wird angezeigt.

   Wenn die Liste nur die Standardzuweisungsregeln enthält, müssen Sie eine neue Zuweisung erstellen.

2. Geben Sie in das Feld **Zuweisungsname** einen Namen ein.

3. Sie können **Agenten-Kriterien** nach dem Speicherort in der Systemstruktur, nach dem Agenten-Subnetz oder individuell wie folgt konfigurieren:

   - Speicherort in der Systemstruktur – Wählen Sie die Gruppe unter **Speicherort in der Systemstruktur** aus.

     Sie können die Systemstruktur durchsuchen, um andere Gruppen aus **Systemstrukturgruppe auswählen** auszuwählen und angezeigte Systemstrukturgruppen mithilfe der Schaltflächen **+** und **-** hinzuzufügen bzw. zu entfernen.

   - Agenten-Subnetz – Geben Sie die IP-Adressen, IP-Bereiche oder Subnetzmasken in das Textfeld ein.

   - Individuell – Geben Sie die IPv4/IPv6-Adresse für ein bestimmtes System in das Textfeld ein.

4. Sie können für die **Steuerungspriorität** entweder **Alle Agentensteuerungen verwenden** oder **Liste benutzerdefinierter Steuerungen verwenden** auswählen. Wenn Sie auf **Liste benutzerdefinierter Steuerungen verwenden** klicken, können Sie die Steuerung wie folgt ändern:
   - Sie können die zugewiesene Steuerung ändern, indem Sie eine weitere Steuerung zur Liste hinzufügen und die vorher zugewiesene Steuerung löschen.
   - Sie können weitere Steuerungen zur Liste hinzufügen und die Priorität festlegen, die der Agent bei der Kommunikation mit den Steuerungen einhält.



Bei Verwendung einer Liste benutzerdefinierter Steuerungen können Sie mit **+** und - weitere Agentensteuerungen zur Liste hinzufügen bzw. aus ihr entfernen (eine Agentensteuerung kann auch in mehreren Gruppen enthalten sein). Ändern Sie die Priorität von Steuerungen mittels Ziehen und Ablegen. Mit welcher Steuerung die Agenten die Kommunikation zuerst versuchen, richtet sich nach der Priorität.

5. Klicken Sie auf **Speichern**.

Gruppieren von Agenten nach Zuweisungspriorität

Fassen Sie Agenten in Gruppen zusammen, und weisen Sie sie einer Agentensteuerung zu, die Zuweisungspriorität verwendet.

Steuerungszuweisungen können angeben, ob eine einzelne Steuerung oder eine Liste von Steuerungen verwendet werden soll. Die von Ihnen angegebene Liste kann aus einzelnen Steuerungen oder Gruppen von Steuerungen bestehen. In dieser Liste ist die Reihenfolge festgelegt, in der Agenten versuchen, mithilfe einer bestimmten Agentensteuerung zu kommunizieren.



Achten Sie beim Zuweisen von Systemen zu Agentensteuerungen auf geographische Nähe, um unnötigen Netzwerkverkehr zu vermeiden.

Vorgehensweise

Definitionen zu Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

1. Klicken Sie auf **Menü** | **Konfiguration** | **Agentensteuerungen**. Die Seite **Agentensteuerung** wird angezeigt.



Wenn die Liste nur die Standardzuweisungsregeln enthält, müssen Sie eine neue Zuweisung erstellen.

2. Bearbeiten Sie die Zuweisungen gemäß den in der Aufgabe *Gruppieren von Agenten mithilfe von Zuweisungsregeln* aufgeführten Schritten.
3. Ändern Sie bei Bedarf die Priorität oder Hierarchie der Zuweisungen, indem Sie auf **Aktionen** | **Priorität bearbeiten** klicken.



Durch Verschieben einer Zuweisung in eine niedrigere Priorität als eine andere Zuweisung entsteht eine Hierarchie, in der die niedrigere Zuweisung ein Teil der höheren Zuweisung ist.

4. Gehen Sie wie nachfolgend beschrieben vor, um die Priorität einer Zuweisung zu ändern, die links in der Spalte **Priorität** angezeigt wird:
   - Per Ziehen und Ablegen – Ziehen Sie die Zeile mit der Zuweisung in der Spalte **Priorität** nach oben oder nach unten.
   - Durch Klicken auf **Zum Anfang** – Klicken Sie im Schnellzugriff auf **Zum Anfang**, um die ausgewählte Zuweisung in die oberste Priorität zu verschieben.
5. Klicken Sie auf **Speichern**, wenn Sie die Prioritäten der Zuweisungen ordnungsgemäß konfiguriert haben.

Gruppieren von Agenten mithilfe der Systemstruktur

Gruppieren Sie Agenten, und weisen Sie ihnen mithilfe der Systemstruktur eine Agentensteuerung zu.

Steuerungszuweisungen können angeben, ob eine einzelne Steuerung oder eine Liste von Steuerungen verwendet werden soll. Die von Ihnen angegebene Liste kann aus einzelnen Steuerungen oder Gruppen von Steuerungen bestehen.



Achten Sie beim Zuweisen von Systemen zu Agentensteuerungen auf geographische Nähe, um unnötigen Netzwerkverkehr zu vermeiden.

Vorgehensweise

Definitionen zu Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

1. Klicken Sie auf **Menü** | **Systeme** | **Systemstruktur** | **Systeme**.
2. Wechseln Sie in der Spalte **Systemstruktur** zu dem System oder zu der Gruppe, das bzw. die Sie verschieben möchten.
3. Ziehen Sie Systeme aus der aktuell konfigurierten Systemgruppe in die gewünschte Systemgruppe.
4. Klicken Sie auf **OK**.

Verwalten Ihrer Netzwerksicherheit

Damit Ihre Organisation vor Bedrohungen geschützt ist, ist es besonders wichtig, dass die McAfee-Produkte immer mit den neuesten Sicherheitsinhalten aktualisiert werden. Der McAfee ePO-Server hilft Ihnen dabei, diese Aktualisierungen auf allen Systemen in Ihrem Netzwerk vorzunehmen.

9 Systemstruktur

Die Systemstruktur ist eine grafische Darstellung der Struktur Ihres verwalteten Netzwerks. Mithilfe von ePolicy Orchestrator können Sie die Strukturierung Ihrer Systeme automatisieren und anpassen. Die von Ihnen festgelegte Organisationsstruktur hat Einfluss darauf, wie Sicherheitsrichtlinien im Netzwerk vererbt und erzwungen werden.

Die Systemstruktur können Sie mittels einer der folgenden Methoden organisieren:

- Durch automatische Synchronisierung mit Ihrem Active Directory- oder NT-Domänen-Server
- Durch kriterienbasierte Sortierung, wobei Kriterien manuell oder automatisch auf Systeme angewendet werden
- Durch manuelle Organisation von der Konsole aus (mittels Ziehen und Ablegen)

Inhalt

Die Systemstruktur

Die Systemstruktur ist eine hierarchische Struktur, die die Systeme aus Ihrem Netzwerk in Gruppen und Untergruppen organisiert.

In der Standardeinstellung enthält die Systemstruktur zwei *Gruppen*:

- *Eigene Organisation* – Der Stamm Ihrer Systemstruktur.
- *Lost&Found (Sammelgruppe)* – Die Erfassungsgruppe für alle Systeme, die nicht zu anderen Gruppen in der Systemstruktur gehören.

Die Gruppe "Eigene Organisation"

Die Stammgruppe "Eigene Organisation" der Systemstruktur enthält alle Systeme, die ihr (manuell oder automatisch) hinzugefügt oder im Netzwerk entdeckt wurden. Solange Sie keine eigene Struktur erstellen, werden alle Systeme zur Lost&Found-Gruppe hinzugefügt.

Die Gruppe "Eigene Organisation" hat die folgenden Eigenschaften:

- Sie kann nicht gelöscht werden.
- Sie kann nicht umbenannt werden.

Die Lost&Found-Gruppe (Sammelgruppe)

Die Lost&Found-Gruppe ist eine Untergruppe der Gruppe "Eigene Organisation". Abhängig von den Methoden, mit denen die Systemstruktur erstellt und verwaltet wird, bestimmt der Server anhand unterschiedlicher Eigenschaften, wo Systeme eingeordnet werden sollen. Die Lost&Found-Gruppe speichert Systeme, deren Standort nicht ermittelt werden konnte.

Die Lost&Found-Gruppe hat folgende Eigenschaften:

- Sie kann nicht gelöscht werden.
- Sie kann nicht umbenannt werden.
- Ihre Sortierungskriterien können nicht so geändert werden, dass sie keine Erfassungsgruppe mehr ist. (Sie können jedoch Sortierungskriterien für die von Ihnen darunter erstellten Untergruppen festlegen.)
- Sie wird immer als letztes Element in der Liste angezeigt und innerhalb gleichrangiger Elemente nicht alphabetisch geordnet.
- Benutzern müssen Berechtigungen für die Lost&Found-Gruppe gewährt werden, um die Inhalte dieser Gruppe anzeigen zu können.
- Wenn ein System in die Lost&Found-Gruppe sortiert wird, wird es in eine Untergruppe abgelegt, die nach der Domäne des Systems benannt ist. Falls diese Gruppe noch nicht vorhanden ist, wird sie erstellt.



Denken Sie beim Entfernen von Systemen aus der Systemstruktur daran, die Option zum Entfernen der zugehörigen Agenten auszuwählen. Falls ein Agent nicht entfernt wird, werden gelöschte Systeme in der Lost&Found-Gruppe wieder angezeigt, weil der Agent weiterhin mit dem Server kommuniziert.

Systemstrukturgruppen

Systemstrukturgruppen stellen Sammlungen von Systemen dar. Welche Systeme zusammen zu gruppieren sind, hängt von den jeweiligen Anforderungen Ihres Netzwerks und Ihres Unternehmens ab. Sie können Systeme nach verschiedenen Kriterien zusammenfassen: nach dem Computertyp (z. B. Laptops, Server oder Desktopcomputer), nach der Region (z. B. Nordamerika oder Europa), nach unterschiedlichen Abteilungen (z. B. Finanzen oder Entwicklung) oder nach anderen Kriterien.

Gruppen haben folgende Eigenschaften:

- Sie werden von Administratoren oder Benutzern mit den entsprechenden Berechtigungen erstellt.
- Sie können sowohl Systeme als auch andere Gruppen (*Untergruppen*) enthalten.
- Sie werden von einem Administrator oder einem Benutzer mit den entsprechenden Berechtigungen verwaltet.

Durch das Gruppieren von Systemen mit ähnlichen Eigenschaften oder Anforderungen in Einheiten können Sie Richtlinien für Systeme zentral verwalten, anstatt die Richtlinien für jedes einzelne System individuell festzulegen.

Zur Planung gehört auch die Organisation der Systeme in Gruppen, bevor Sie mit dem Erstellen der Systemstruktur beginnen.

Vererbung

Vererbung ist eine wichtige Eigenschaft, die das Verwalten von Richtlinien und Tasks vereinfacht. Durch Vererbung übernehmen in der Systemstrukturhierarchie untergeordnete Gruppen Richtlinien, die für ihre übergeordneten Gruppen festgelegt wurden, z. B.:

- Richtlinien, die auf der Ebene "Eigene Organisation" festgelegt wurden, werden an darunter liegende Gruppen vererbt.
- Untergruppen oder einzelne Systeme erben die Richtlinien ihrer Gruppen.

Die Vererbung ist standardmäßig für alle Gruppen und einzelnen Systeme aktiviert, die Sie zur Systemstruktur hinzufügen. Dadurch müssen Sie an weniger Punkten Richtlinien festlegen und Client-Tasks planen.

Die Vererbung kann jedoch bei Bedarf durch Zuordnen einer neuen Richtlinie an einer beliebigen Stelle der Systemstruktur unterbrochen werden (vorausgesetzt, der Benutzer verfügt über die erforderlichen Berechtigungen). Zur Beibehaltung der Vererbung können Sie Richtlinienzuweisungen sperren.

Erwägungen beim Planen der Systemstruktur

Eine effiziente und gut organisierte Systemstruktur kann die Wartung vereinfachen. Der Aufbau der Systemstruktur wird von vielen administrativen, netzwerkbedingten und politischen Gegebenheiten einer Umgebung beeinflusst.

Planen Sie daher die Organisation der Systemstruktur, bevor Sie sie erstellen und auffüllen. Besonders bei großen Netzwerken wäre der Aufwand für das mehrfache Erstellen der Systemstruktur erheblich.

Da jedes Netzwerk anders ist und unterschiedliche Richtlinien erfordert (möglicherweise sogar eine unterschiedliche Verwaltung), sollten Sie die Systemstruktur planen, bevor Sie die McAfee ePO-Software einrichten.

Unabhängig von den Methoden, die Sie zum Erstellen und Auffüllen der Systemstruktur verwenden, sollten Sie beim Planen der Systemstruktur Ihre Umgebung berücksichtigen.

Administratorzugriff

Wenn Sie die Organisation der Systemstruktur planen, sollten Sie die Anforderungen an den Benutzerzugriff der Personen berücksichtigen, die das System verwalten werden.

Möglicherweise verfügt Ihr Unternehmen über eine dezentralisierte Netzwerkverwaltung, bei der unterschiedliche Administratoren die Verantwortung für unterschiedliche Teile des Netzwerks tragen. Aus Sicherheitsgründen dürfen Sie möglicherweise kein Administratorkonto verwenden, das Zugriff auf alle Teile Ihres Netzwerks hat. In diesem Szenario dürfen Sie mit einem einzelnen Administratorkonto keine Richtlinien festlegen und keine Agenten ausbringen. Stattdessen müssen Sie die Systemstruktur möglicherweise auf Grundlage der Abteilungen in Gruppen organisieren und Konten und Berechtigungssätze erstellen.

Berücksichtigen Sie die folgenden Fragen:

- Wer ist für die Verwaltung welcher Systeme verantwortlich?
- Wer benötigt Zugriff auf Informationen zu diesen Systemen?
- Wer sollte Zugriff auf die Systeme und die Informationen dazu besitzen?

Diese Fragen haben sowohl Einfluss auf die Organisation der Systemstruktur als auch auf die Berechtigungssätze, die Sie erstellen und auf Benutzerkonten anwenden.

Gliederung der Umgebung und ihr Einfluss auf die Systemorganisation

Die Art der Organisation der Systeme für die Verwaltung hängt von der Gliederung ab, die in Ihrem Netzwerk gilt. Diese Gliederung beeinflusst den Aufbau der Systemstruktur auf andere Weise als den Aufbau Ihrer Netzwerktopologie.

Sie sollten folgende Gliederungsarten in Ihrem Netzwerk und in Ihrem Unternehmen sowie die Frage beurteilen, ob diese beim Aufbau der Systemstruktur berücksichtigt werden müssen.

Topologische Gliederung

Das Netzwerk ist bereits durch NT-Domänen oder Active Directory-Container definiert. Je besser die Netzwerkumgebung organisiert ist, desto einfacher ist es, die Systemstruktur mit den Synchronisierungsfunktionen zu erstellen und zu verwalten.

Geographische Gliederung

Die Verwaltung der Sicherheit ist eine ständige Balance zwischen Schutz und Leistung. Bauen Sie die Systemstruktur so auf, dass die begrenzte Bandbreite bestmöglich genutzt wird. Beachten Sie, wie sich der Server mit allen Teilen Ihres Netzwerks verbindet. Vor allem Remote-Standorte sind oft nur über langsame WAN- oder VPN-Verbindungen statt schnellerer LAN-Verbindungen angeschlossen. Um den Netzwerkverkehr über langsamere Verbindungen zu verringern, sollten Sie Richtlinien für Aktualisierung und Agent-zu-Server-Kommunikation für Remote-Standorte anders konfigurieren.

Das Anordnen von Systemen nach geographischen Gesichtspunkten bietet verschiedene Vorteile beim Konfigurieren von Richtlinien:

- Sie können Aktualisierungsrichtlinien für die Gruppe so konfigurieren, dass sich alle Systeme von mindestens einem nahe gelegenen verteilten Software-Repository aktualisieren.
- Sie können Client-Tasks so planen, dass sie zu Zeiten ausgeführt werden, die für den jeweiligen Standort besser geeignet sind.

Politische Gliederung

Viele große Netzwerke sind nach Personen oder Gruppen unterteilt, die unterschiedliche Teile des Netzwerks verwalten. Manchmal stimmt diese Gliederung nicht mit der topologischen oder geographischen Gliederung überein. Die Auswahl der Personen, die auf die Segmente der Systemstruktur zugreifen und sie verwalten, beeinflusst deren Strukturierung.

Funktionale Gliederung

Einige Netzwerke werden nach den Rollen der Netzwerknutzer unterteilt, zum Beispiel die Vertriebs- und die Entwicklungsabteilung. Selbst wenn das Netzwerk nicht funktional gegliedert ist, müssen Sie Teile der Systemstruktur möglicherweise nach Funktion organisieren, wenn verschiedene Gruppen unterschiedliche Richtlinien benötigen.

Eine Geschäftsgruppe kann spezifische Software verwenden, die spezielle Sicherheitsrichtlinien erfordert. Sie können zum Beispiel die E-Mail-Exchange-Server in einer Gruppe anordnen und bestimmte Ausschlüsse für On-Access-Scans durch McAfee® VirusScan® Enterprise festlegen.

Subnetze und IP-Adressbereiche

In vielen Fällen werden für Organisationseinheiten eines Netzwerks bestimmte Subnetze oder IP-Bereiche verwendet, weshalb Sie für einen geographischen Standort eine Gruppe erstellen und mindestens einen IP-Filter dafür festlegen können. Wenn Ihr Netzwerk jedoch nicht über mehrere

geographische Standorte verteilt ist, können Sie als primäres Gliederungskriterium Informationen zum Netzwerkstandort verwenden, z. B. IP-Adressen.



Sie sollten nach Möglichkeit auf IP-Adressinformationen basierende Sortierungskriterien zur Automatisierung der Systemstrukturerstellung und -wartung verwenden. Legen Sie Kriterien für IP-Subnetzmasken oder IP-Adressbereiche für mögliche Gruppen in der Systemstruktur fest. Diese Filter füllen Speicherorte automatisch mit den entsprechenden Systemen auf.

Betriebssysteme und Software

Systeme mit ähnlichen Betriebssystemen können Sie in Gruppen zusammenfassen, um das Verwalten betriebssystemspezifischer Produkte und Richtlinien zu vereinfachen. Wenn Sie über ältere Systeme verfügen, können Sie dafür eine Gruppe erstellen und Sicherheitsprodukte auf diesen Systemen separat ausbringen und verwalten. Indem Sie diesen Systemen ein entsprechendes Tag zuweisen, können Sie sie außerdem automatisch in eine Gruppe sortieren.

Tags und Systeme mit ähnlichen Eigenschaften

Sie können Tags für die automatische Sortierung in Gruppen verwenden. Tags identifizieren Systeme mit ähnlichen Eigenschaften. Wenn Sie Ihre Gruppen anhand von Eigenschaften organisieren können, haben Sie die Möglichkeit, auf diesen Kriterien basierende Tags zu erstellen und zuzuordnen und diese Tags als Gruppensortierungskriterien zu verwenden. Auf diese Weise stellen Sie sicher, dass die Systeme automatisch in die entsprechenden Gruppen sortiert werden.

Sie sollten nach Möglichkeit auf Tag-basierte Sortierungskriterien verwenden, um die Gruppen mit den entsprechenden Systemen aufzufüllen.

Active Directory- und NT-Domänensynchronisierung

Die Software ePolicy Orchestrator kann in Active Directory- sowie NT-Domänen als Quelle für Systeme integriert werden und Active Directory als Quelle für die Gliederung der Systemstruktur verwenden.

Active Directory-Synchronisierung

Wenn das Netzwerk Active Directory ausführt, können Sie die gesamte Systemstruktur oder Teile davon mit der Active Directory-Synchronisierung erstellen, auffüllen und verwalten.

Nachdem die Systemstruktur definiert wurde, wird sie mit neuen Systemen (und Untercontainern) in Active Directory aktualisiert.

Active Directory-Integration ermöglicht Ihnen Folgendes:

- Synchronisierung mit Ihrer Active Directory-Struktur durch Importieren von Systemen und Active Directory-Untercontainern (als Systemstrukturgruppen) sowie Aktualisieren mit Active Directory. Bei jeder Synchronisierung werden die Systeme und die Struktur in der Systemstruktur aktualisiert, um die Systeme und die Struktur von Active Directory widerzuspiegeln.
- Importieren von Systemen als unsortierte Liste aus dem Active Directory-Container (und seinen Untercontainern) in die synchronisierte Gruppe.
- Steuern der Vorgehensweise bei potenziell doppelten Systemen.
- Verwenden der Systembeschreibung, die zusammen mit den Systemen aus Active Directory importiert wird.

In früheren Versionen von ePolicy Orchestrator standen zwei Tasks zur Verfügung: Active Directory-Import und Active Directory-Entdeckung. Gehen Sie jetzt wie nachfolgend beschrieben vor, um die Systemstruktur in Ihre Active Directory-Systemstruktur zu integrieren:

1. Konfigurieren Sie die Synchronisierungseinstellungen in jeder Gruppe, die einen Zuordnungspunkt in der Systemstruktur darstellt. An derselben Stelle können Sie konfigurieren, ob:
   - Agenten auf entdeckte Systeme ausgebracht werden sollen.
   - Systeme beim Löschen in Active Directory auch in der Systemstruktur gelöscht werden sollen.
   - Doppelte Einträge von Systemen, die an einer anderen Stelle in der Systemstruktur vorhanden sind, zugelassen werden sollen.
2. Importieren Sie die Active Directory-Systeme (und gegebenenfalls die Struktur) entsprechend den Synchronisierungseinstellungen mit der Aktion "Jetzt synchronisieren" in die Systemstruktur.
3. Verwenden Sie den Server-Task "NT-Domänen-/Active Directory-Synchronisierung", um die Systeme (und gegebenenfalls die Active Directory-Struktur) entsprechend den Synchronisierungseinstellungen regelmäßig mit der Systemstruktur zu synchronisieren.

Typen der Active Directory-Synchronisierung

Es gibt zwei Typen der Active Directory-Synchronisierung (*Nur Systeme* sowie *Systeme und Struktur*). Je nachdem, wie weit Sie Active Directory integrieren möchten, können Sie sich für eine Variante entscheiden.

Bei beiden Typen steuern Sie die Synchronisierung durch die Auswahl folgender Optionen:

- Automatisches Ausbringen von Agenten auf Systemen, die in ePolicy Orchestrator neu sind. Diese Einstellung sollten Sie nicht für die erste Synchronisierung festlegen, wenn Sie eine große Anzahl an Systemen importieren und nur eine begrenzte Bandbreite zur Verfügung steht. Die Agenten-MSI-Datei hat eine Größe von ca. 6 MB. Möglicherweise möchten Sie Agenten jedoch bei späteren Synchronisierungen automatisch auf neuen Systemen ausbringen, die in Active Directory erkannt werden.
- Löschen von Systemen von ePolicy Orchestrator (und entfernen ihrer Agenten), wenn sie in Active Directory gelöscht werden.
- Verhindern, dass Systeme zur Gruppe hinzugefügt werden, wenn sie bereits an einer anderen Stelle der Systemstruktur vorhanden sind. Damit stellen Sie sicher, dass beim manuellen Verschieben oder Sortieren von Systemen keine doppelten Systeme erstellt werden.
- Ausschließen bestimmter Active Directory-Container aus der Synchronisierung. Diese Container und ihre Systeme werden bei der Synchronisierung ignoriert.

Systeme und Struktur

Wenn Sie diesen Synchronisierungstyp verwenden, werden Änderungen an der Active Directory-Struktur bei der nächsten Synchronisierung in die Systemstruktur übernommen. Beim Hinzufügen, Ändern oder Entfernen von Systemen oder Containern in Active Directory werden diese an den entsprechenden Stellen der Systemstruktur ebenfalls hinzugefügt, geändert oder entfernt.

Verwendung dieses Synchronisierungstyps

Mithilfe dieses Synchronisierungstyps stellen Sie sicher, dass die Systemstruktur (oder Teile davon) Ihrer Active Directory-Struktur genau gleichen.

Wenn die Organisation von Active Directory Ihre Anforderungen an die Sicherheitsverwaltung erfüllt und die Systemstruktur weiterhin der zugewiesenen Active Directory-Struktur gleichen soll, verwenden Sie diesen Synchronisierungstyp bei nachfolgenden Synchronisierungen.

Nur Systeme

Mit diesem Synchronisierungstyp können Sie Systeme aus einem Active Directory-Container (und aus nicht ausgeschlossenen Untercontainern) als unsortierte Liste in eine zugewiesene Systemstrukturgruppe importieren. Anschließend können Sie die Systeme an die entsprechenden Stellen in der Systemstruktur verschieben, indem Sie Gruppen Sortierungskriterien zuweisen.

Wenn Sie sich für diesen Synchronisierungstyp entscheiden, müssen Sie sich vergewissern, dass Sie keine Systeme erneut hinzufügen, die bereits an einer anderen Stelle in der Systemstruktur vorhanden sind. Auf diese Weise vermeiden Sie doppelte Einträge in der Systemstruktur.

Verwendung dieses Synchronisierungstyps

Verwenden Sie diesen Synchronisierungstyp, wenn Sie Active Directory als Standardquelle für ePolicy Orchestrator verwenden und die Unternehmensanforderungen an die Sicherheitsverwaltung sich nicht mit der Organisation der Container und Systeme in Active Directory vereinbaren lassen.

NT-Domänensynchronisierung

Verwenden Sie Ihre NT-Domänen als Ausgangspunkt für das Auffüllen der Systemstruktur. Wenn Sie eine Gruppe mit einer NT-Domäne synchronisieren, werden alle Systeme dieser Domäne als unsortierte Liste in der Gruppe abgelegt. Sie können diese Systeme in einer einzelnen Gruppe verwalten oder zur genaueren Gliederung Untergruppen erstellen. Mithilfe einer Methode wie der automatischen Sortierung können Sie diese Untergruppen automatisch auffüllen.

Wenn Sie Systeme in andere Gruppen oder Untergruppen der Systemstruktur verschieben, stellen Sie sicher, dass Sie die Systeme nicht hinzufügen, wenn sie an anderer Stelle der Systemstruktur bereits vorhanden sind. Auf diese Weise vermeiden Sie doppelte Einträge in der Systemstruktur.

Anders als bei der Active Directory-Synchronisierung werden bei der NT-Domänensynchronisierung nur die Systemnamen synchronisiert. Die Systembeschreibung wird nicht synchronisiert.

Kriterienbasierte Sortierung

Wie in den früheren Versionen von ePolicy Orchestrator können Sie verwaltete Systeme mithilfe von IP-Adressinformationen automatisch in bestimmte Gruppen sortieren. Sie können auch Tag-basierte Sortierungskriterien erstellen, die Systemen zugewiesenen Beschriftungen ähneln. Um sicherzustellen, dass sich Systeme an der gewünschten Stelle in der Systemstruktur befinden, können Sie entweder einen der Kriterientypen oder beide verwenden.

Systeme müssen nur ein Kriterium der Sortierungskriterien einer Gruppe erfüllen, um der Gruppe zugeordnet zu werden.

Führen Sie nach dem Erstellen von Gruppen und dem Festlegen Ihrer Sortierungskriterien einen Sortiertest aus, um zu überprüfen, ob die Kriterien und die Sortierreihenfolge die gewünschten Ergebnisse erzielen.

Sobald Sie Sortierungskriterien zu Ihren Gruppen hinzugefügt haben, können Sie die Aktion "Jetzt sortieren" ausführen. Diese Aktion verschiebt die ausgewählten Systeme automatisch in die entsprechende Gruppe. Systeme, die den Sortierungskriterien keiner Gruppe entsprechen, werden in die Sammelgruppe verschoben.

Neue Systeme, die sich zum ersten Mal beim Server anmelden, werden automatisch in die richtige Gruppe verschoben. Wenn Sie die Sortierungskriterien jedoch nach der ersten Agent-zu-Server-Kommunikation definieren, müssen Sie für diese Systeme die Aktion "Jetzt sortieren" ausführen, um sie sofort in die entsprechende Gruppe zu verschieben. Sie können jedoch auch bis zur nächsten Agent-zu-Server-Kommunikation warten.

Sortierungsstatus der Systeme

Sie können die Systemstruktursortierung für jedes System oder für jede Sammlung von Systemen aktivieren bzw. deaktivieren. Wenn Sie die Systemstruktursortierung bei einem System deaktivieren, wird es von allen Sortieraktionen bis auf den Sortiertest ausgeschlossen. Beim einem Sortiertest wird der Sortierstatus des Systems oder der Sammlung betrachtet, und das System kann auf der Seite **Sortiertest** verschoben oder sortiert werden.

Einstellungen der Systemstruktursortierung auf dem McAfee ePO-Server

Die Sortierung kann nur ausgeführt werden, wenn die Sortierfunktion auf dem Server und auf den Systemen aktiviert ist. Standardmäßig ist das einmalige Sortieren von Systemen aktiviert. Daher werden Systeme bei der ersten Agent-zu-Server-Kommunikation (oder dann, wenn an vorhandenen Systemen Änderungen vorgenommen werden) sortiert, und danach nicht wieder.

Systemsortiertest

Mit dieser Funktion können Sie anzeigen, wo Systeme bei einer Sortierungsaktion abgelegt werden würden. Auf der Seite **Sortiertest** werden die Systeme und die Pfade der Speicherorte angezeigt, an denen sie einsortiert werden würden. Zwar wird der Sortierungsstatus der Systeme auf dieser Seite nicht angezeigt, doch wenn Sie Systeme auf der Seite auswählen (selbst solche mit deaktivierter Sortierung) und auf **Systeme verschieben** klicken, werden die Systeme am angegebenen Speicherort abgelegt.

Auswirkung von Einstellungen auf die Sortierung

Sie können zwischen drei Server-Einstellungen wählen, die bestimmen, ob und wann Systeme sortiert werden. Außerdem können Sie wählen, ob ein System sortiert werden kann, indem Sie die Systemstruktursortierung für ausgewählte Systeme in der Systemstruktur aktivieren oder deaktivieren.

Server-Einstellungen

Der Server verfügt über drei Einstellungen:

- **Systemstruktursortierung deaktivieren** – Wenn eine kriterienbasierte Sortierung Ihre Anforderungen an die Sicherheitsverwaltung nicht erfüllt und Sie Ihre Systeme mit anderen Systemstrukturfunktionen (wie der Active Directory-Synchronisierung) organisieren möchten, wählen Sie diese Einstellung, damit andere McAfee ePO-Benutzer nicht versehentlich Sortierungskriterien für Gruppen konfigurieren und Systeme an unerwünschte Speicherorte verschieben.
- **Systeme bei jeder Agent-zu-Server-Kommunikation sortieren** – Die Systeme werden bei jeder Agent-zu-Server-Kommunikation erneut sortiert. Wenn Sie die Sortierungskriterien für Gruppen ändern, werden die Systeme bei der nächsten Agent-zu-Server-Kommunikation in die neue Gruppe verschoben.
- **Systeme einmal sortieren** – Die Systeme werden bei der nächsten Agent-zu-Server-Kommunikation sortiert und dann gekennzeichnet, sodass sie bei Agent-zu-Server-Kommunikationen nicht mehr sortiert werden, so lange diese Einstellung ausgewählt ist. Sie können ein solches System jedoch sortieren, indem Sie es markieren und auf **Jetzt sortieren** klicken.

Systemeinstellungen

Sie können die Systemstruktursortierung für jedes System deaktivieren oder aktivieren. Wenn die Systemstruktursortierung auf einem System deaktiviert ist, wird dieses System nicht sortiert, unabhängig davon, welche Sortierungsaktion ausgeführt wird. Bei der Aktion "Jetzt sortieren" wird

dieses System jedoch sortiert. Bei aktivierter Systemstruktursortierung wird das betreffende System bei der manuellen Aktion "Jetzt sortieren" und – je nach den Server-Einstellungen für die Systemstruktursortierung – bei der Agent-zu-Server-Kommunikation sortiert.

Kriterien für die IP-Adressensortierung

In vielen Netzwerken geben die Subnetze und IP-Adressinformationen Hinweise auf die Unternehmensstruktur (z. B. auf geographische Standorte oder Aufgaben). Wenn die Organisation der IP-Adressen Ihren Anforderungen entspricht, sollten Sie die Systemstruktur oder Teile davon mithilfe dieser Informationen erstellen und verwalten, indem Sie Kriterien für die IP-Adressensortierung für solche Gruppen festlegen.

In der vorliegenden Version von ePolicy Orchestrator wurde diese Funktion geändert, und Sie haben jetzt die Möglichkeit, IP-Sortierungskriterien an jedem beliebigen Punkt in der Struktur festzulegen. Sie müssen nicht mehr darauf achten, dass die Kriterien der IP-Adressensortierung der untergeordneten Gruppe eine Teilmenge der Kriterien der übergeordneten Gruppe sind (sofern der übergeordneten Gruppe keine Kriterien zugewiesen sind). Sobald die Funktion konfiguriert ist, können Sie Systeme bei einer Agent-zu-Server-Kommunikation oder nur bei einer manuell ausgelösten Sortierungsaktion sortieren.



Die Kriterien für die IP-Adressensortierung sollten sich zwischen den einzelnen Gruppen nicht überschneiden. Jeder IP-Bereich oder jede IP-Subnetzmaske in den Sortierungskriterien einer Gruppe sollte eine eindeutige Menge an IP-Adressen abdecken. Wenn sich Kriterien überschneiden, hängt es von der Reihenfolge der Untergruppen auf der Registerkarte **Systemstruktur | Gruppeninformationen** ab, in welche Gruppe diese Systeme sortiert werden. Mit der Aktion **IP-Integrität überprüfen** auf der Registerkarte **Gruppeninformationen** können Sie IP-Adressen auf Überscheidungen überprüfen.

Tag-basierte Sortierungskriterien

Sie können nicht nur Systeme mithilfe von IP-Adressinformationen in die entsprechende Gruppe sortieren, sondern auch Sortierungskriterien anhand der den Systemen zugewiesenen Tags definieren.

Tag-basierte Kriterien können zusammen mit auf IP-Adressen basierenden Kriterien für die Sortierung genutzt werden.

Gruppenreihenfolge und -sortierung

Zusätzliche Flexibilität bei der Systemstrukturverwaltung erhalten Sie, indem Sie die Reihenfolge der Untergruppen einer Gruppe konfigurieren. Damit legen Sie auch die Reihenfolge fest, in der diese Untergruppen beim Sortieren für eine Einordnung des Systems in Betracht gezogen werden.

Wenn mehrere Untergruppen übereinstimmende Kriterien besitzen, kann die Änderung dieser Reihenfolge die Position eines Systems in der Systemstruktur ändern.

Wenn Sie Erfassungsgruppen verwenden, müssen diese außerdem die letzte Untergruppe in der Liste sein.

Erfassungsgruppen

Bei Erfassungsgruppen handelt es sich um Gruppen, deren Sortierungskriterien auf der Seite **Sortierungskriterien** der Gruppe auf **Alle anderen** eingestellt sind. Nur Untergruppen an der letzten Stelle der Sortierreihenfolge können Erfassungsgruppen sein. Diese Gruppen erhalten alle Systeme, die in die übergeordnete Gruppe, aber in keine der gleichrangigen Gruppen der Erfassungsgruppe sortiert wurden.

Tags

Inhalt

Erstellen von Tags mit dem Tag-Generator

Mit dem neuen Assistenten **Tag-Generator** können Sie Tags schnell erstellen.

Tags können Kriterien verwenden, auf die hin jedes System bewertet wird:

- Automatisch bei der Agent-zu-Server-Kommunikation.
- Wenn die Aktion "Tag-Kriterien ausführen" ausgeführt wird.
- Manuell auf ausgewählten Systemen mit der Aktion "Tag anwenden", unabhängig von den Kriterien.

Tags ohne Kriterien können nur manuell auf ausgewählte Systeme angewendet werden.

Vorgehensweise

Definitionen zu Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

1. Klicken Sie auf **Menü** | **Systeme** | **Tag-Katalog**, und klicken Sie dann auf **Tag-Aktionen** | **Neues Tag**. Der Assistent **Tag-Generator** wird angezeigt.
2. Geben Sie auf der Seite **Beschreibung** einen Namen und eine eindeutige Beschreibung ein, und klicken Sie anschließend auf **Weiter**. Die Seite **Kriterien** wird angezeigt.
3. Wählen Sie die gewünschten Kriterien aus, und konfigurieren Sie diese. Klicken Sie anschließend auf **Weiter**. Die Seite **Test** wird angezeigt.

   Wenn das Tag automatisch angewendet werden soll, müssen Sie Kriterien für das Tag konfigurieren.

4. Legen Sie fest, ob Systeme nur bei der Aktion "Tag-Kriterien ausführen" oder auch bei jeder Agent-zu-Server-Kommunikation anhand der Tag-Kriterien bewertet werden sollen. Klicken Sie anschließend auf **Weiter**. Die Seite **Vorschau** wird angezeigt.

   Diese Optionen sind nur verfügbar, wenn Kriterien konfiguriert wurden. Beim Bewerten von Systemen anhand von Tag-Kriterien wird das Tag auf Systeme angewendet, die die Kriterien erfüllen und nicht von diesem Tag ausgeschlossen wurden.

5. Überprüfen Sie die Informationen auf dieser Seite, und klicken Sie dann auf **Speichern**.

   Wenn das Tag über Kriterien verfügt, wird auf dieser Seite die Anzahl an Systemen angezeigt, die dieses Tag beim Bewerten anhand der Tag-Kriterien erhalten.

Das Tag wird auf der Seite **Tag-Katalog** zur Tag-Liste hinzugefügt.

Planmäßiges Anwenden von kriterienbasierten Tags

Sie können einen regelmäßigen Task planen, der ein Tag auf alle Systeme anwendet, die die Tag-Kriterien erfüllen.

Vorgehensweise

Definitionen zu Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

1. Klicken Sie auf **Menü** | **Automatisierung** | **Server-Tasks**, und klicken Sie dann auf **Aktionen** | **Neuer Task**. Die Seite **Generator für Server-Tasks** wird angezeigt.
2. Geben Sie auf der Seite **Beschreibung** einen Namen und eine Beschreibung für den Task ein, wählen Sie aus, ob der Task bei der Erstellung aktiviert wird, und klicken Sie dann auf **Weiter**. Die Seite **Aktionen** wird angezeigt.
3. Wählen Sie in der Dropdown-Liste die Option **Tag-Kriterien ausführen** aus, und wählen Sie anschließend in der Dropdown-Liste **Tag** ein Tag aus.
4. Legen Sie fest, ob manuell gekennzeichnete oder ausgeschlossene Systeme zurückgesetzt werden sollen.



Beim Zurücksetzen manuell mit Tags versehener und ausgeschlossener Systeme wird das Tag von Systemen entfernt, die nicht mit den Kriterien übereinstimmen, während das Tag auf die Systeme angewendet wird, die mit den Kriterien übereinstimmen, aber vom Erhalt des Tags ausgeschlossen wurden.

5. Klicken Sie auf **Weiter**, um die Seite **Plan** zu öffnen.
6. Planen Sie den Task für die gewünschten Zeiten ein, und klicken Sie dann auf **Weiter**.
7. Überprüfen Sie die Task-Einstellungen, und klicken Sie dann auf **Speichern**.

Der Server-Task wird zur Liste auf der Seite **Server-Tasks** hinzugefügt. Wenn Sie den Task im Assistenten **Generator für Server-Tasks** aktiviert haben, wird er zum nächsten geplanten Zeitpunkt ausgeführt.

Ausschließen von Systemen von der automatischen Kennzeichnung

Sie können Systeme von der Anwendung bestimmter Tags ausschließen.



Wahlweise können Sie Systeme auch mit einer Abfrage erfassen und die gewünschten Tags dann mithilfe der Abfrageergebnisse von diesen Systemen ausschließen.

Vorgehensweise

Definitionen zu Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

1. Klicken Sie auf **Menü** | **Systeme** | **Systemstruktur** | **Systeme**, und wählen Sie dann die Gruppe aus, die die Systeme in der Systemstruktur enthält.
2. Wählen Sie in der Tabelle **Systeme** mindestens ein System aus, und klicken Sie dann auf **Aktionen** | **Tag** | **Tag ausschließen**.
3. Wählen Sie im Dialogfeld **Tag ausschließen** in der Dropdown-Liste das gewünschte Tag aus, das aus den ausgewählten Systemen ausgeschlossen werden soll, und klicken Sie dann auf **OK**.

4 Überprüfen Sie die Systeme, die vom Tag ausgeschlossen wurden:

   a Klicken Sie auf **Menü** | **Systeme** | **Tag-Katalog**, und wählen Sie dann das gewünschte Tag in der Tag-Liste aus.

   b Klicken Sie im Detailbereich neben **Systeme mit Tag** auf den Link, um die Anzahl der von der kriterienbasierten Tag-Anwendung ausgeschlossenen Systeme zu erhalten. Die Seite **Vom Tag ausgeschlossene Systeme** wird angezeigt.

   c Vergewissern Sie sich, dass sich die gewünschten Systeme in der Liste befinden.

Anwenden von Tags auf ausgewählte Systeme

Sie können ein Tag manuell auf ausgewählte Systeme in der Systemstruktur anwenden.

Vorgehensweise

Definitionen zu Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

1 Klicken Sie auf **Menü** | **Systeme** | **Systemstruktur** | **Systeme**, und wählen Sie dann die Gruppe mit dem gewünschten System aus.

2 Wählen Sie die gewünschten Systeme aus, und klicken Sie dann auf **Aktionen** | **Tag** | **Tag anwenden**.

3 Wählen Sie im Dialogfeld **Tag anwenden** in der Dropdown-Liste das gewünschte Tag aus, das auf die ausgewählten Systeme angewendet werden soll, und klicken Sie dann auf **OK**.

4 Überprüfen Sie, ob die Tags angewendet wurden:

   a Klicken Sie auf **Menü** | **Systeme** | **Tag-Katalog**, und wählen Sie dann das gewünschte Tag in der Tag-Liste aus.

   b Klicken Sie im Detailbereich neben **Systeme mit Tag** auf den Link, um die Anzahl der manuell gekennzeichneten Systeme zu erhalten. Die Seite **Systeme mit manuell angewendetem Tag** wird angezeigt.

   c Vergewissern Sie sich, dass sich die gewünschten Systeme in der Liste befinden.

Automatisches Anwenden von kriterienbasierten Tags auf alle übereinstimmenden Systeme

Gehen Sie wie in diesen Aufgaben beschrieben vor, um kriterienbasierte Tags automatisch auf alle Systeme anzuwenden, die die Kriterien erfüllen.

Aufgaben

- *Anwenden von kriterienbasierten Tags auf alle übereinstimmenden Systeme* auf Seite 118
  Sie können ein kriterienbasiertes Tag auf alle nicht ausgeschlossenen Systeme anwenden, die mit den angegebenen Kriterien übereinstimmen.
- *Planmäßiges Anwenden von kriterienbasierten Tags* auf Seite 116
  Sie können einen regelmäßigen Task planen, der ein Tag auf alle Systeme anwendet, die die Tag-Kriterien erfüllen.

Anwenden von kriterienbasierten Tags auf alle übereinstimmenden Systeme

Sie können ein kriterienbasiertes Tag auf alle nicht ausgeschlossenen Systeme anwenden, die mit den angegebenen Kriterien übereinstimmen.

Vorgehensweise

Definitionen zu Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

1. Klicken Sie auf **Menü** | **Systeme** | **Tag-Katalog**, und wählen Sie dann ein Tag in der Tag-Liste aus.
2. Klicken Sie auf **Aktionen** | **Tag-Kriterien ausführen**.
3. Legen Sie im Bereich **Aktion** fest, ob Sie manuell gekennzeichnete oder ausgeschlossene Systeme zurücksetzen möchten.

   Beim Zurücksetzen manuell mit Tags versehener und ausgeschlossener Systeme wird das Tag von Systemen entfernt, die nicht mit den Kriterien übereinstimmen, während das Tag auf die Systeme angewendet wird, die mit den Kriterien übereinstimmen, aber vom Erhalt des Tags ausgeschlossen wurden.

4. Klicken Sie auf **OK**.
5. Überprüfen Sie, ob das Tag auf die Systeme angewendet wurde:
   a. Klicken Sie auf **Menü** | **Systeme** | **Tag-Katalog**, und wählen Sie dann das gewünschte Tag in der Tag-Liste aus.
   b. Klicken Sie im Detailbereich neben **Systeme mit Tag** auf den Link, um die Anzahl der Systeme mit nach Kriterien angewendeten Tags zu erhalten. Die Seite **Systeme mit nach Kriterien angewendetem Tag** wird angezeigt.
   c. Vergewissern Sie sich, dass sich die gewünschten Systeme in der Liste befinden.

Das Tag wird auf alle Systeme angewendet, die seine Kriterien erfüllen.

Planmäßiges Anwenden von kriterienbasierten Tags

Sie können einen regelmäßigen Task planen, der ein Tag auf alle Systeme anwendet, die die Tag-Kriterien erfüllen.

Vorgehensweise

Definitionen zu Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

1. Klicken Sie auf **Menü** | **Automatisierung** | **Server-Tasks**, und klicken Sie dann auf **Aktionen** | **Neuer Task**. Die Seite **Generator für Server-Tasks** wird angezeigt.
2. Geben Sie auf der Seite **Beschreibung** einen Namen und eine Beschreibung für den Task ein, wählen Sie aus, ob der Task bei der Erstellung aktiviert wird, und klicken Sie dann auf **Weiter**. Die Seite **Aktionen** wird angezeigt.
3. Wählen Sie in der Dropdown-Liste die Option **Tag-Kriterien ausführen** aus, und wählen Sie anschließend in der Dropdown-Liste **Tag** ein Tag aus.
4. Legen Sie fest, ob manuell gekennzeichnete oder ausgeschlossene Systeme zurückgesetzt werden sollen.

   Beim Zurücksetzen manuell mit Tags versehener und ausgeschlossener Systeme wird das Tag von Systemen entfernt, die nicht mit den Kriterien übereinstimmen, während das Tag auf die Systeme angewendet wird, die mit den Kriterien übereinstimmen, aber vom Erhalt des Tags ausgeschlossen wurden.

5. Klicken Sie auf **Weiter**, um die Seite **Plan** zu öffnen.
6. Planen Sie den Task für die gewünschten Zeiten ein, und klicken Sie dann auf **Weiter**.
7. Überprüfen Sie die Task-Einstellungen, und klicken Sie dann auf **Speichern**.

Der Server-Task wird zur Liste auf der Seite **Server-Tasks** hinzugefügt. Wenn Sie den Task im Assistenten **Generator für Server-Tasks** aktiviert haben, wird er zum nächsten geplanten Zeitpunkt ausgeführt.

Hinzufügen eines Systems zur Systemstruktur bei aktivierter Sortierung

Wenn der Agent zum ersten Mal mit dem Server kommuniziert, ordnet der Server das System mithilfe eines Algorithmus in die Systemstruktur ein. Systeme, für die kein geeigneter Speicherort gefunden wird, werden in die Lost&Found-Gruppe (Sammelgruppe) abgelegt.

Bei jeder Agent-zu-Server-Kommunikation versucht der Server, das System anhand der Agenten-GUID in der Systemstruktur zu finden. (Es verfügen nur die Systeme über eine Agenten-GUID in der Datenbank, deren Agenten sich bereits zum ersten Mal beim Server gemeldet haben.) Falls ein übereinstimmendes System gefunden wird, verbleibt es in seinem vorhandenen Speicherort.

Wenn kein übereinstimmendes System gefunden wird, sortiert der Server die Systeme mithilfe eines Algorithmus in die entsprechenden Gruppen. Die Systeme können in eine beliebige kriterienbasierte Gruppe in der Systemstruktur eingeordnet werden, egal wie tief die Gruppe in der Struktur angeordnet ist. Voraussetzung dafür ist, dass keine übergeordnete Gruppe des Pfads nicht übereinstimmende Kriterien besitzt. Übergeordnete Gruppen einer kriterienbasierten Untergruppe müssen entweder keine Kriterien oder übereinstimmende Kriterien haben.

Die den einzelnen Untergruppen zugewiesene Sortierreihenfolge (die auf der Registerkarte **Gruppeninformationen** definiert ist) bestimmt, in welcher Reihenfolge diese Untergruppen vom Server berücksichtigt werden, wenn nach einer Gruppe mit übereinstimmenden Kriterien gesucht wird.

1. Der Server sucht in einer Gruppe, die denselben Namen wie die Domäne trägt, nach einem System ohne Agenten-GUID (der Agent des Systems hat sich noch nie gemeldet) mit einem übereinstimmenden Namen. Wenn ein System gefunden wird, wird es in diese Gruppe eingeordnet. Dieser Vorgang kann bei der ersten Active Directory- oder NT-Domänensynchronisierung erfolgen oder wenn Sie Systeme manuell zur Systemstruktur hinzugefügt haben.
2. Wenn kein übereinstimmendes System gefunden wird, sucht der Server nach einer Gruppe, die denselben Namen wie die Domäne trägt, aus der das System stammt. Wird keine solche Gruppe gefunden, wird sie innerhalb der Lost&Found-Gruppe erstellt, und das System wird zu dieser Gruppe hinzugefügt.
3. Die Eigenschaften des Systems werden aktualisiert.
4. Wenn der Server so konfiguriert ist, dass er die Sortierungskriterien bei jeder Agent-zu-Server-Kommunikation ausführt, wendet er alle kriterienbasierten Tags auf das System an.
5. Die weiteren Schritte hängen davon ab, ob die Systemstruktursortierung sowohl auf dem Server als auch auf dem System aktiviert ist.
   - Wenn die Systemstruktursortierung entweder auf dem Server oder dem System deaktiviert ist, wird das System in seinem derzeitigen Speicherort belassen.
   - Bei aktivierter Systemstruktursortierung auf dem Server und dem System wird das System basierend auf den Sortierungskriterien in die Systemstrukturgruppen verschoben.

   Bei Systemen, die während der Active Directory- oder NT-Domänensynchronisierung hinzugefügt wurden, ist die Systemstruktursortierung standardmäßig deaktiviert, sodass sie bei der ersten Agent-zu-Server-Kommunikation nicht sortiert werden.
6. Der Server berücksichtigt die Sortierungskriterien aller übergeordneten Gruppen entsprechend der Sortierreihenfolge auf der Registerkarte **Gruppeninformationen** der Gruppe **Eigene Organisation**. Das System

wird vom Server zur ersten Gruppe mit übereinstimmenden Kriterien oder zu einer Erfassungsgruppe zugeordnet, die er berücksichtigt.

- Sobald ein System einer Gruppe zugeordnet ist, werden alle seine Untergruppen entsprechend ihrer Sortierreihenfolge auf der Registerkarte **Gruppeninformationen** auf übereinstimmende Kriterien überprüft.
- Dieser Vorgang wird so lange ausgeführt, bis keine Untergruppe mit übereinstimmenden Kriterien für das System vorhanden ist und es der letzten gefundenen Gruppe mit übereinstimmenden Kriterien zugeordnet wird.

7. Wenn keine übergeordnete Gruppe gefunden wird, werden die Untergruppen von übergeordneten Gruppen (ohne Sortierungskriterien) entsprechend ihrer Sortierung berücksichtigt.
8. Wenn keine solche kriterienbasierte Gruppe der zweiten Ebene gefunden wird, werden die kriterienbasierten Gruppen der dritten Ebene aus den uneingeschränkten Gruppen der zweiten Ebene berücksichtigt.



Untergruppen von Gruppen mit nicht übereinstimmenden Kriterien werden nicht berücksichtigt. Eine Gruppe muss übereinstimmende Kriterien oder keine Kriterien besitzen, damit ihre Untergruppen für ein System berücksichtigt werden.

9. Auf diese Weise wird die Systemstruktur abwärts durchlaufen, bis ein System in eine Gruppe einsortiert ist.



Wenn die Server-Einstellung für die Systemstruktursortierung so konfiguriert ist, dass eine Sortierung nur bei der ersten Agent-zu-Server-Kommunikation erfolgt, wird das System entsprechend gekennzeichnet. Diese Kennzeichnung bedeutet, dass das System erst dann wieder bei einer Agent-zu-Server-Kommunikation sortiert werden kann, wenn die Server-Einstellung so geändert wird, dass das Sortieren bei jeder Agent-zu-Server-Kommunikation möglich ist.

10. Wenn der Server das System keiner Gruppe zuordnen kann, wird es in die Lost&Found-Gruppe in einer Untergruppe mit dem Namen seiner Domäne eingeordnet.

Aktivieren der Systemstruktursortierung auf dem Server

Die Systeme werden nur sortiert, wenn die Systemstruktursortierung sowohl auf dem Server als auch auf den gewünschten Systemen aktiviert ist.

Vorgehensweise

Definitionen zu Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

1. Klicken Sie auf **Menü** | **Konfiguration** | **Server-Einstellungen**, wählen Sie in der Liste **Einstellungskategorien** den Eintrag **Systemstruktursortierung** aus, und klicken Sie dann auf **Bearbeiten**.
2. Legen Sie fest, ob Systeme nur bei der ersten oder bei jeder Agent-zu-Server-Kommunikation sortiert werden sollen.

Wenn Sie festgelegt haben, dass nur bei der ersten Agent-zu-Server-Kommunikation sortiert werden soll, werden alle aktivierten Systeme bei ihrer nächsten Agent-zu-Server-Kommunikation sortiert. Anschließend werden sie so lange nicht sortiert, wie diese Option ausgewählt ist. Sie können diese Systeme jedoch manuell erneut sortieren, indem Sie die Aktion "Jetzt sortieren" ausführen oder diese Einstellung so ändern, dass bei jeder Agent-zu-Server-Kommunikation sortiert wird.

Wenn Sie festgelegt haben, dass bei jeder Agent-zu-Server-Kommunikation sortiert werden soll, werden alle aktivierten Systeme so lange bei jeder Agent-zu-Server-Kommunikation sortiert, wie diese Option ausgewählt ist.

Erstellen und Auffüllen von Systemstrukturgruppen

Sie können Systemstrukturgruppen erstellen und diese mit Systemen auffüllen, indem Sie für einzelne Systeme die NetBIOS-Namen eingeben oder Systeme direkt aus dem Netzwerk importieren.



Außerdem können Sie auch ausgewählte Systeme in beliebige Gruppen in der Systemstruktur ziehen, um Gruppen aufzufüllen. Auf diese Weise können Sie Gruppen und Untergruppen auch innerhalb der Systemstruktur verschieben.

Es gibt viele verschiedene Möglichkeiten, eine Systemstruktur zu organisieren. Da sich jedes Netzwerk unterscheidet, kann Ihre Systemstrukturorganisation ebenso einmalig sein wie Ihr Netzwerklayout. Obwohl Sie nicht alle verfügbaren Methoden verwenden werden, können Sie mehrere einsetzen.

Wenn Sie zum Beispiel Active Directory in Ihrem Netzwerk verwenden, können Sie Ihre Active Directory-Container anstelle der NT-Domänen importieren. Wenn die Organisation Ihrer Active Directory- oder NT-Domänen für die Sicherheitsverwaltung nicht in Frage kommen, können Sie die Organisation Ihrer Systemstruktur in einer Textdatei erstellen und sie dann in die Systemstruktur importieren. Wenn Ihr Netzwerk kleiner ist, können Sie die Systemstruktur manuell erstellen und jedes System manuell hinzufügen.

Aufgaben

- *Manuelles Erstellen von Gruppen* auf Seite 123
  Sie können manuell Untergruppen in der Systemstruktur erstellen. Dabei können Sie diese Gruppen mit Systemen auffüllen, indem Sie für einzelne Systeme die NetBIOS-Namen eingeben oder Systeme direkt aus dem Netzwerk importieren.
- *Manuelles Hinzufügen von Systemen zu einer vorhandenen Gruppe* auf Seite 123
  Sie können Systeme aus der Netzwerkumgebung in Gruppen importieren. Darüber hinaus können Sie eine Netzwerkdomäne oder einen Active Directory-Container importieren.
- *Exportieren von Systemen aus der Systemstruktur* auf Seite 124
  Sie können eine Liste von Systemen aus der Systemstruktur in eine TXT-Datei exportieren, um sie später zu verwenden. Der Export erfolgt auf Gruppen- oder Untergruppenebene unter Beibehaltung der Positionen in der Systemstruktur.
- *Importieren von Systemen aus einer Textdatei* auf Seite 125
  Sie können eine Textdatei mit einer Liste von Systemen und Gruppen für den Import in die Systemstruktur erstellen.
- *Sortieren von Systemen in kriterienbasierten Gruppen* auf Seite 126
  Sie können die Sortierung für die Gruppierung von Systemen konfigurieren und implementieren. Damit Systeme in Gruppen sortiert werden, muss die Sortierung auf dem Server und den gewünschten Systemen aktiviert sein. Außerdem müssen Sortierungskriterien und die Sortierreihenfolge der Gruppen konfiguriert sein.
- *Importieren von Active Directory-Containern* auf Seite 128
  Sie können Systeme aus Active Directory-Containern direkt in Ihre Systemstruktur importieren, indem Sie die Active Directory-Quellcontainer den Systemstrukturgruppen zuordnen.
- *Importieren von NT-Domänen in eine vorhandene Gruppe* auf Seite 130
  Sie können Systeme aus einer NT-Domäne in eine manuell erstellte Gruppe importieren.
- *Planen der Systemstruktursynchronisierung* auf Seite 132
  Sie können einen Server-Task planen, der die Systemstruktur mit Änderungen in der zugeordneten Domäne oder dem zugeordneten Active Directory-Container aktualisiert.
- *Manuelles Aktualisieren einer synchronisierten Gruppe mit einer NT-Domäne* auf Seite 133
  Aktualisieren Sie eine synchronisierte Gruppe mit Änderungen in der zugehörigen NT-Domäne.

Manuelles Erstellen von Gruppen

Sie können manuell Untergruppen in der Systemstruktur erstellen. Dabei können Sie diese Gruppen mit Systemen auffüllen, indem Sie für einzelne Systeme die NetBIOS-Namen eingeben oder Systeme direkt aus dem Netzwerk importieren.

Vorgehensweise

Definitionen zu Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

1. Wählen Sie die gewünschte Gruppe in der Systemstruktur aus, unter der eine Untergruppe erstellt werden soll. Führen Sie dann Folgendes durch:
   - Klicken Sie auf der Seite **Gruppeninformationen** (unter **Menü** | **Systeme** | **Systemstruktur** | **Gruppeninformationen**) auf **Aktionen** | **Neue Untergruppe**.
   - Klicken Sie auf der Seite **Systemstruktur** (unter **Menü** | **Systeme** | **Systemstruktur**) auf **Systemstrukturaktionen** | **Neue Untergruppe**.
2. Das Dialogfeld **Neue Untergruppe** wird angezeigt.

    Sie können auch mehrere Untergruppen gleichzeitig erstellen.

3. Geben Sie den gewünschten Namen ein, und klicken Sie dann auf **OK**. Die neue Gruppe wird in der Systemstruktur angezeigt.
4. Wiederholen Sie diesen Schritt so lange, bis Sie die Gruppen mit den gewünschten Systemen auffüllen können. Sie haben folgende Möglichkeiten, Systeme zur Systemstruktur hinzuzufügen und sicherzustellen, dass sie in die gewünschten Gruppen eingeordnet werden:
   - Manuelles Eingeben der Systemnamen.
   - Importieren aus NT-Domänen oder Active Directory-Containern. Zur einfacheren Verwaltung können Sie eine Domäne oder einen Container regelmäßig mit einer Gruppe synchronisieren.
   - Einrichten von IP-Adressen- oder Tag-basierten Sortierungskriterien für die Gruppen. Wenn Agenten von Systemen mit übereinstimmenden IP-Adressinformationen oder Tags einchecken, werden sie automatisch in die entsprechende Gruppe eingeordnet.

Manuelles Hinzufügen von Systemen zu einer vorhandenen Gruppe

Sie können Systeme aus der Netzwerkumgebung in Gruppen importieren. Darüber hinaus können Sie eine Netzwerkdomäne oder einen Active Directory-Container importieren.

Vorgehensweise

Definitionen zu Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

1. Klicken Sie auf **Menü** | **Systeme** | **Systemstruktur**, und klicken Sie dann im Menü **Systemstrukturaktionen** auf **Neue Systeme**. Die Seite **Neue Systeme** wird angezeigt.
2. Legen Sie fest, ob der Agent auf die neuen Systeme ausgebracht werden soll und ob die Systeme zur ausgewählten Gruppe oder entsprechend den Sortierungskriterien zu einer Gruppe hinzugefügt werden sollen.
3. Geben Sie neben **Zielsysteme** den NetBIOS-Namen für die einzelnen Systeme in das Textfeld ein, und trennen Sie diese mit Kommas, Leerzeichen oder Zeilenumbrüchen. Klicken Sie alternativ auf **Durchsuchen**, um die Systeme auszuwählen.

4 Wenn Sie die Option **Agenten pushen und Systeme zur aktuellen Gruppe hinzufügen** ausgewählt haben, können Sie die automatische Systemstruktursortierung aktivieren. Hiermit wenden Sie die Sortierungskriterien auf diese Systeme an.

Geben Sie die folgenden Optionen an:

Option	Aktion
Agenten-Version	Wählen Sie die auszubringende Agenten-Version aus.
Installationspfad	Konfigurieren Sie den Agenten-Installationspfad, oder übernehmen Sie den Standardpfad.
Anmeldeinformationen für Agenten-Installation	Geben Sie gültige Anmeldeinformationen ein, um den Agenten zu installieren.
Anzahl der Versuche	Geben Sie einen ganzzahligen Wert ein, wobei 0 für beliebig viele Versuche steht.
Wiederholungsintervall	Geben Sie die Anzahl der Sekunden zwischen Wiederholungen ein.
Abbrechen nach	Geben Sie die Anzahl der Minuten ein, nach denen die Verbindung abgebrochen wird.
Agenten pushen mit	Wählen Sie entweder eine bestimmte Agentensteuerung oder alle Agentensteuerungen aus.

5 Klicken Sie auf **OK**.

Exportieren von Systemen aus der Systemstruktur

Sie können eine Liste von Systemen aus der Systemstruktur in eine TXT-Datei exportieren, um sie später zu verwenden. Der Export erfolgt auf Gruppen- oder Untergruppenebene unter Beibehaltung der Positionen in der Systemstruktur.

Es kann nützlich sein, über eine Liste der Systeme aus der Systemstruktur zu verfügen. Sie können diese Liste in den McAfee ePO-Server importieren, um eine frühere Struktur und Anordnung schnell wiederherzustellen.



Die Systeme werden hierbei nicht aus der Systemstruktur entfernt. Es wird eine TXT-Datei erstellt, die die Namen und Struktur von Systemen in der Systemstruktur enthält.

Vorgehensweise

Definitionen zu Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

1 Klicken Sie auf **Menü** | **Systeme** | **Systemstruktur**. Die Seite **Systemstruktur** wird geöffnet.

2 Wählen Sie die Gruppe oder Untergruppe aus, in der sich die zu exportierenden Systeme befinden, und klicken Sie dann auf **Systemstrukturaktionen** | **Systeme exportieren**. Die Seite **Systeme exportieren** wird geöffnet.

3 Wählen Sie aus, welche Elemente exportiert werden sollen:

- **Allen Systemen in dieser Gruppe** – Exportiert die Systeme in der angegebenen **Quellgruppe**, jedoch keine Systeme, die sich in unterhalb dieser Ebene verschachtelten Untergruppen befinden.
- **Allen Systemen in dieser Gruppe und Untergruppen** – Exportiert alle auf und unterhalb dieser Ebene befindlichen Systeme.

4 Klicken Sie auf **OK**.

Die Seite **Exportieren** wird geöffnet. Sie können auf den Link **Systeme** klicken, um die Systemliste anzuzeigen, oder mit der rechten Maustaste auf den Link klicken, um eine Kopie der Datei **EXPORTSYSTEMS.TXT** zu speichern.

Importieren von Systemen aus einer Textdatei

Sie können eine Textdatei mit einer Liste von Systemen und Gruppen für den Import in die Systemstruktur erstellen.

Aufgaben

- *Erstellen einer Textdatei mit Gruppen und Systemen* auf Seite 125
  Sie können eine Textdatei mit den NetBIOS-Namen Ihrer Netzwerksysteme erstellen, die Sie in eine Gruppe importieren möchten. Dabei haben Sie die Möglichkeit, eine unsortierte Liste von Systemen zu importieren oder die Systeme in Gruppen zu unterteilen.
- *Importieren von Systemen und Gruppen aus einer Textdatei* auf Seite 125
  Sie können Systeme oder Systemgruppen aus einer Textdatei, die Sie erstellt und gespeichert haben, in die Systemstruktur importieren.

Erstellen einer Textdatei mit Gruppen und Systemen

Sie können eine Textdatei mit den NetBIOS-Namen Ihrer Netzwerksysteme erstellen, die Sie in eine Gruppe importieren möchten. Dabei haben Sie die Möglichkeit, eine unsortierte Liste von Systemen zu importieren oder die Systeme in Gruppen zu unterteilen.

Definieren Sie die Gruppen und deren Systeme, indem Sie die Gruppen- und Systemnamen in eine Textdatei eingeben. Importieren Sie diese Informationen dann in ePolicy Orchestrator. Bei größeren Netzwerken müssen Sie Netzwerkdienstprogramme verwenden (z. B. das zum Microsoft Windows Resource Kit gehörige NETDOM.EXE), um Textdateien mit vollständigen Listen der Systeme in Ihrem Netzwerk zu erstellen. Sobald die Textdatei erstellt ist, können Sie sie manuell bearbeiten, um Gruppen von Systemen zu erstellen und die gesamte Struktur in die Systemstruktur zu importieren.

Unabhängig davon, wie Sie die Textdatei erstellen, müssen Sie die richtige Syntax verwenden, bevor Sie sie importieren.

Vorgehensweise

1. Jedes System muss auf einer separaten Zeile aufgeführt sein. Um die Systeme in Gruppen aufzuteilen, geben Sie den Gruppennamen gefolgt von einem umgekehrten Schrägstrich (\ ) ein, und führen Sie darunter die dazu gehörigen Systeme auf, wobei jedes System auf einer eigenen Zeile steht.

   ```
   GruppeA\System1

   GruppeA\System2

   GruppeA\GruppeB\System3

   GruppeC\GruppeD
   ```

2. Vergewissern Sie sich, dass die Namen der Gruppen und Systeme sowie die Syntax der Textdatei korrekt sind. Speichern Sie anschließend die Textdatei in einem temporären Ordner auf dem Server.

Importieren von Systemen und Gruppen aus einer Textdatei

Sie können Systeme oder Systemgruppen aus einer Textdatei, die Sie erstellt und gespeichert haben, in die Systemstruktur importieren.

Definitionen zu Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

Vorgehensweise

1. Klicken Sie auf **Menü** | **Systeme** | **Systemstruktur**. Klicken Sie dann auf **Systemstrukturaktionen**, und wählen Sie **Neue Systeme** aus. Die Seite **Neue Systeme** wird angezeigt.

2. Wählen Sie **Systeme aus einer Textdatei in die ausgewählte Gruppe importieren, aber Agenten nicht pushen** aus.

3 Wählen Sie aus, ob die Importdatei folgende Elemente enthält:
   - **Systeme und Systemstruktur**
   - **Nur Systeme (als unsortierte Liste)**
4 Klicken Sie auf **Durchsuchen**, und wählen Sie die Textdatei aus.
5 Legen Sie fest, wie mit Systemen verfahren werden soll, die bereits an anderen Stellen in der Systemstruktur vorhanden sind.
6 Klicken Sie auf **OK**.

Die Systeme werden in die ausgewählte Gruppe in der Systemstruktur importiert. Wenn die Systeme in der Textdatei in Gruppen sortiert sind, werden vom Server Gruppen erstellt und die Systeme importiert.

Sortieren von Systemen in kriterienbasierten Gruppen

Sie können die Sortierung für die Gruppierung von Systemen konfigurieren und implementieren. Damit Systeme in Gruppen sortiert werden, muss die Sortierung auf dem Server und den gewünschten Systemen aktiviert sein. Außerdem müssen Sortierungskriterien und die Sortierreihenfolge der Gruppen konfiguriert sein.

Aufgaben

- *Hinzufügen von Sortierungskriterien zu Gruppen* auf Seite 126
  Sortierungskriterien für Systemstrukturgruppen können auf IP-Adressinformationen oder Tags basieren.
- *Aktivieren der Systemstruktursortierung auf dem Server* auf Seite 121
  Die Systeme werden nur sortiert, wenn die Systemstruktursortierung sowohl auf dem Server als auch auf den gewünschten Systemen aktiviert ist.
- *Aktivieren oder Deaktivieren der Systemstruktursortierung auf Systemen* auf Seite 127
  Der Sortierungsstatus eines Systems bestimmt, ob es in eine kriterienbasierte Gruppe sortiert werden kann.
- *Manuelles Sortieren von Systemen* auf Seite 128
  Sie können ausgewählte Systeme mit aktivierter kriterienbasierter Sortierung in Gruppen sortieren.

Hinzufügen von Sortierungskriterien zu Gruppen

Sortierungskriterien für Systemstrukturgruppen können auf IP-Adressinformationen oder Tags basieren.

Vorgehensweise

Definitionen zu Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

1 Klicken Sie auf **Menü | Systeme | Systemstruktur | Gruppeninformationen**, und wählen Sie dann in der Systemstruktur die Gruppe aus.
2 Klicken Sie neben **Sortierungskriterien** auf **Bearbeiten**. Die Seite **Sortierungskriterien** für die ausgewählte Gruppe wird angezeigt.
3 Wählen Sie **Systeme, die mit einem der unten stehenden Sortierungskriterien übereinstimmen** aus. Die Kriterienauswahl wird angezeigt.



Obwohl Sie mehrere Sortierungskriterien für die Gruppe konfigurieren können, muss ein System nur ein einziges Kriterium erfüllen, um in diese Gruppe eingeordnet zu werden.

4 Konfigurieren Sie das Kriterium. Folgende Optionen stehen zur Auswahl:
   - **IP-Adressen** – Definieren Sie in diesem Textfeld einen IP-Adressbereich oder eine IP-Subnetzmaske als Sortierungskriterium. Jedes System, dessen Adresse sich in diesem Bereich befindet, wird in diese Gruppe sortiert.
   - **Tags** – Fügen Sie spezifische Tags hinzu, damit Systeme mit diesen Tags, die in die übergeordnete Gruppe eingeordnet werden, in diese Gruppe sortiert werden.
5 Wiederholen Sie diesen Vorgang so lange, bis die Sortierungskriterien für die Gruppe konfiguriert sind, und klicken Sie dann auf **Speichern**.

Aktivieren der Systemstruktursortierung auf dem Server

Die Systeme werden nur sortiert, wenn die Systemstruktursortierung sowohl auf dem Server als auch auf den gewünschten Systemen aktiviert ist.

Vorgehensweise

Definitionen zu Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

1. Klicken Sie auf **Menü** | **Konfiguration** | **Server-Einstellungen**, wählen Sie in der Liste **Einstellungskategorien** den Eintrag **Systemstruktursortierung** aus, und klicken Sie dann auf **Bearbeiten.**
2. Legen Sie fest, ob Systeme nur bei der ersten oder bei jeder Agent-zu-Server-Kommunikation sortiert werden sollen.

Wenn Sie festgelegt haben, dass nur bei der ersten Agent-zu-Server-Kommunikation sortiert werden soll, werden alle aktivierten Systeme bei ihrer nächsten Agent-zu-Server-Kommunikation sortiert. Anschließend werden sie so lange nicht sortiert, wie diese Option ausgewählt ist. Sie können diese Systeme jedoch manuell erneut sortieren, indem Sie die Aktion "Jetzt sortieren" ausführen oder diese Einstellung so ändern, dass bei jeder Agent-zu-Server-Kommunikation sortiert wird.

Wenn Sie festgelegt haben, dass bei jeder Agent-zu-Server-Kommunikation sortiert werden soll, werden alle aktivierten Systeme so lange bei jeder Agent-zu-Server-Kommunikation sortiert, wie diese Option ausgewählt ist.

Aktivieren oder Deaktivieren der Systemstruktursortierung auf Systemen

Der Sortierungsstatus eines Systems bestimmt, ob es in eine kriterienbasierte Gruppe sortiert werden kann.

Sie können den Sortierungsstatus auf Systemen in jeder beliebigen Tabelle mit Systemen (z. B. Abfrageergebnisse) sowie automatisch bei den Ergebnissen einer geplanten Abfrage ändern.

Definitionen zu Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

Vorgehensweise

1. Klicken Sie auf **Menü** | **Systeme** | **Systemstruktur** | **Systeme**, und wählen Sie dann das gewünschte System aus.
2. Klicken Sie auf **Aktionen** | **Verzeichnisverwaltung** | **Sortierungsstatus ändern**, und legen Sie dann fest, ob die Systemstruktursortierung auf ausgewählten Systemen aktiviert oder deaktiviert werden soll.
3. Legen Sie im Dialogfeld **Sortierungsstatus ändern** fest, ob die Systemstruktursortierung auf dem ausgewählten System aktiviert oder deaktiviert werden soll.



Je nach der Server-Einstellung für die Systemstruktursortierung werden diese Systeme bei der nächsten Agent-zu-Server-Kommunikation sortiert. Andernfalls können sie nur mit der Aktion "Jetzt sortieren" sortiert werden.

Manuelles Sortieren von Systemen

Sie können ausgewählte Systeme mit aktivierter kriterienbasierter Sortierung in Gruppen sortieren.

Vorgehensweise

Definitionen zu Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

1. Klicken Sie auf **Menü** | **Systeme** | **Systemstruktur** | **Systeme**, und wählen Sie dann die Gruppe mit den gewünschten Systemen aus.
2. Wählen Sie die Systeme aus, und klicken Sie dann auf **Aktionen** | **Verzeichnisverwaltung** | **Jetzt sortieren**. Das Dialogfeld **Jetzt sortieren** wird angezeigt.

   Wenn Sie vor dem Sortieren eine Vorschau der Ergebnisse anzeigen möchten, klicken Sie auf **Sortiertest**. (Wenn Sie Systeme auf der Seite **Sortiertest** verschieben, werden jedoch alle ausgewählten Systeme sortiert, auch wenn die Systemstruktursortierung für sie deaktiviert ist.)

3. Klicken Sie auf **OK**, um die Systeme zu sortieren.

Importieren von Active Directory-Containern

Sie können Systeme aus Active Directory-Containern direkt in Ihre Systemstruktur importieren, indem Sie die Active Directory-Quellcontainer den Systemstrukturgruppen zuordnen.

Durch Zuordnen von Active Directory-Containern zu Gruppen ist Folgendes möglich:

- Synchronisieren der Systemstruktur mit der Active Directory-Struktur, sodass beim Hinzufügen oder Entfernen von Containern in Active Directory die entsprechende Gruppe in der Systemstruktur ebenfalls hinzugefügt oder entfernt wird
- Löschen von Systemen in der Systemstruktur, wenn sie in Active Directory gelöscht werden
- Vermeiden von doppelten Systemeinträgen in der Systemstruktur, wenn sie bereits in anderen Gruppen vorhanden sind

Definitionen zu Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

Vorgehensweise

1. Klicken Sie auf **Menü** | **Systeme** | **Systemstruktur** | **Gruppeninformationen**, und wählen Sie dann in der Systemstruktur die gewünschte Gruppe aus. Wählen Sie dabei die Gruppe aus, der Sie einen Active Directory-Container zuordnen möchten.

   Die Lost&Found-Gruppe (Sammelgruppe) der Systemstruktur kann nicht synchronisiert werden.

2. Klicken Sie neben **Synchronisierungstyp** auf **Bearbeiten**. Die Seite **Synchronisierungseinstellungen** für die ausgewählte Gruppe wird angezeigt.
3. Klicken Sie neben **Synchronisierungstyp** auf **Active Directory**. Die Optionen für die Active Directory-Synchronisierung werden angezeigt.

4 Legen Sie den Typ der Active Directory-Synchronisierung fest, die zwischen dieser Gruppe und dem gewünschten Active Directory-Container (und seinen Untercontainern) stattfinden soll:

- **Systeme und Containerstruktur** – Wählen Sie diese Option, wenn diese Gruppe die Active Directory-Struktur vollständig widerspiegeln soll. Bei der Synchronisierung wird die Systemstruktur dieser Gruppe geändert, um die Struktur des Active Directory-Containers widerzuspiegeln, dem sie zugeordnet ist. Container, die in Active Directory hinzugefügt oder daraus entfernt werden, werden auch zur Systemstruktur hinzugefügt bzw. aus ihr entfernt. Wenn Systeme in Active Directory hinzugefügt, verschoben oder entfernt werden, werden sie auch zur Systemstruktur hinzugefügt bzw. in ihr vorschoben oder aus ihr entfernt.

- **Nur Systeme (als unsortierte Liste)** – Wählen Sie diese Option, wenn allein diese Gruppe ausschließlich mit Systemen aus dem Active Directory-Container (und nicht ausgeschlossenen Untercontainern) gefüllt werden soll. Beim Spiegeln von Active Directory werden keine Untergruppen erstellt.

5 Wählen Sie aus, ob für ein System, das bereits in einer anderen Gruppe der Systemstruktur vorhanden ist, ein doppelter Eintrag erstellt werden soll.



Die Auswahl dieser Option wird insbesondere dann nicht empfohlen, wenn Sie die Active Directory-Synchronisierung nur als Ausgangspunkt für die Sicherheitsverwaltung verwenden möchten und für die weitere Feinabstimmung der Organisation unterhalb des Zuordnungspunkts andere Funktionen zur Systemstrukturverwaltung (z. B. Tag-Sortierung) nutzen.

6 Unter **Active Directory-Domäne** können Sie folgende Aktionen durchführen:

- Geben Sie den vollqualifizierten Domänennamen der Active Directory-Domäne ein.
- Wählen Sie in einer Liste bereits registrierter LDAP-Server einen LDAP-Server aus.

7 Klicken Sie neben **Container** auf **Hinzufügen**. Wählen Sie im Dialogfeld **Active Directory-Container auswählen** einen Quellcontainer aus, und klicken Sie auf **OK**.

8 Klicken Sie zum Ausschließen bestimmter Untercontainer neben **Ausnahmen** auf **Hinzufügen**, und wählen Sie die auszuschließenden Untercontainer aus. Klicken Sie anschließend auf **OK**.

9 Wählen Sie aus, ob Agenten automatisch auf neuen Systemen ausgebracht werden sollen. Wenn Sie diese Option auswählen, müssen Sie auch die Ausbringungseinstellungen konfigurieren.



Sie sollten den Agenten nicht während des Erstimports eines großen Containers ausbringen. Das gleichzeitige Ausbringen des 3,62 MB großen Agenten-Pakets auf viele Systeme kann zu einer Überlastung des Netzwerks führen. Stattdessen sollten Sie den Container importieren und den Agenten anschließend in Systemgruppen ausbringen, anstatt alle Systeme auf einmal zu kontaktieren. Sie sollten diese Seite erneut aufrufen und diese Option nach der ersten Agenten-Ausbringung auswählen, damit der Agent automatisch auf neu zu Active Directory hinzugefügten Systemen installiert wird.

10 Legen Sie fest, ob Systeme beim Löschen in der Active Directory-Domäne auch in der Systemstruktur gelöscht werden sollen. Optional können Sie festlegen, ob Agenten von den gelöschten Systemen entfernt werden sollen.

11 Um die Gruppe sofort mit Active Directory zu synchronisieren, klicken Sie auf **Jetzt synchronisieren**.

Wenn Sie auf **Jetzt synchronisieren** klicken, werden alle an den Synchronisierungseinstellungen vorgenommenen Änderungen gespeichert, bevor die Gruppe synchronisiert wird. Wenn eine Benachrichtigungsregel für die Active Directory-Synchronisierung aktiviert ist, wird bei jedem hinzugefügten oder entfernten System ein Ereignis generiert (diese Ereignisse werden im Audit-Protokoll angezeigt und können abgefragt werden). Wenn Sie Agenten auf hinzugefügten Systemen ausbringen, wird die Ausbringung für jedes hinzugefügte System ausgeführt. Nach Abschluss der Synchronisierung wird das Feld **Letzte Synchronisierung** aktualisiert. Darin werden die Uhrzeit und das Datum der Synchronisierung und nicht der Zeitpunkt von abgeschlossenen Agenten-Ausbringungen angezeigt.



Wahlweise können Sie für die erste Synchronisierung einen Server-Task "NT-Domänen-/Active Directory-Synchronisierung" planen. Dies ist besonders dann nützlich, wenn Sie Agenten während der ersten Synchronisierung auf neuen Systemen ausbringen und die Bandbreite ein Problem darstellt.

12 Zeigen Sie nach Abschluss der Synchronisierung die Ergebnisse in der Systemstruktur an.

Bringen Sie nach dem Importieren der Systeme die Agenten auf ihnen aus, sofern Sie keine automatische Ausbringung festgelegt haben. Außerdem kann es sinnvoll sein, einen regelmäßigen Server-Task "NT-Domänen-/Active Directory-Synchronisierung" einzurichten, damit die Systemstruktur mit allen neuen Systemen oder Änderungen an der Organisation in Ihren Active Directory-Containern aktualisiert wird.

Importieren von NT-Domänen in eine vorhandene Gruppe

Sie können Systeme aus einer NT-Domäne in eine manuell erstellte Gruppe importieren.

Sie können Gruppen automatisch auffüllen, indem Sie ganze NT-Domänen mit bestimmten Gruppen synchronisieren. Mit dieser Vorgehensweise können Sie in einem Schritt sämtliche Systeme in Ihrem Netzwerk als unsortierte Liste ohne Systembeschreibung zur Systemstruktur hinzufügen.

Wenn die Domäne sehr groß ist, können Sie Untergruppen erstellen, wodurch die Richtlinienverwaltung und die Organisation der Systemstruktur vereinfacht wird. Importieren Sie dazu zuerst die Domäne in eine Gruppe der Systemstruktur, und erstellen Sie dann manuell logische Untergruppen.



Importieren Sie zum Verwalten derselben Richtlinie in mehreren Domänen jede der Domänen in eine Untergruppe innerhalb derselben Gruppe, für die Sie Richtlinien festlegen können, die dann von jeder Untergruppe geerbt werden.

Beachten Sie bei dieser Vorgehensweise Folgendes:

- Legen Sie für Untergruppen IP-Adressen- oder Tag-basierte Sortierungskriterien fest, um die importierten Systeme automatisch zu sortieren.
- Planen Sie zur einfacheren Wartung einen regelmäßigen Server-Task "NT-Domänen-/Active Directory-Synchronisierung".

Definitionen zu Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

Vorgehensweise

1 Klicken Sie auf **Menü** | **Systeme** | **Systemstruktur** | **Gruppeninformationen**, und wählen Sie dann unter **Systemstruktur** eine Gruppe aus bzw. erstellen eine neue Gruppe.

2 Klicken Sie neben **Synchronisierungstyp** auf **Bearbeiten**. Die Seite **Synchronisierungseinstellungen** für die ausgewählte Gruppe wird angezeigt.

3. Klicken Sie neben **Synchronisierungstyp** auf **NT-Domäne**. Die Einstellungen für die Domänensynchronisierung werden angezeigt.
4. Legen Sie neben **Systeme, die an anderen Stellen in der Systemstruktur vorhanden sind** fest, wie mit Systemen verfahren werden soll, die bei der Synchronisierung hinzugefügt werden würden, die aber bereits in einer anderen Gruppe der Systemstruktur vorhanden sind.



Es wird nicht empfohlen, die Option **Systeme zur synchronisierten Gruppe hinzufügen und sie im aktuellen Speicherort in der Systemstruktur belassen** auszuwählen. Das gilt insbesondere dann, wenn Sie die NT-Domänensynchronisierung nur als Ausgangspunkt für die Sicherheitsverwaltung verwenden und für die weitere Feinabstimmung der Organisation unterhalb des Zuordnungspunkts andere Funktionen zur Systemstrukturverwaltung (z. B. Tag-Sortierung) nutzen.

5. Klicken Sie neben **Domäne** auf **Durchsuchen**, und wählen Sie die NT-Domäne aus, die Sie dieser Gruppe zuordnen möchten. Klicken Sie dann auf **OK**. Alternativ können Sie den Namen der Domäne direkt in das Textfeld eingeben.



Geben Sie nicht den vollständigen Domänennamen ein.

6. Wählen Sie aus, ob Agenten automatisch auf neuen Systemen ausgebracht werden sollen. Wenn Sie diese Option auswählen, müssen Sie auch die Ausbringungseinstellungen konfigurieren.



Sie sollten den Agenten nicht während des Erstimports einer großen Domäne ausbringen. Das gleichzeitige Ausbringen des 3,62 MB großen Agenten-Pakets auf viele Systeme kann zu einer Überlastung des Netzwerks führen. Stattdessen sollten Sie die Domäne importieren und den Agenten anschließend in kleineren Systemgruppen ausbringen, anstatt alle Systeme auf einmal zu kontaktieren. Nachdem die Agenten ausgebracht sind, sollten Sie diese Seite erneut aufrufen und diese Option nach der ersten Agenten-Ausbringung auswählen, damit der Agent automatisch per Domänensynchronisierung auf allen neu zur Gruppe (oder ihren Untergruppen) hinzugefügten Systemen installiert wird.

7. Legen Sie fest, ob Systeme beim Löschen in der NT-Domäne auch in der Systemstruktur gelöscht werden sollen. Optional können Sie festlegen, ob Agenten von den gelöschten Systemen entfernt werden sollen.
8. Um die Gruppe sofort mit der Domäne zu synchronisieren, klicken Sie auf **Jetzt synchronisieren**, und warten Sie dann, bis die Systeme in der Domäne zur Gruppe hinzugefügt wurden.



Wenn Sie auf **Jetzt synchronisieren** klicken, werden an den Synchronisierungseinstellungen vorgenommenen Änderungen gespeichert, bevor die Gruppe synchronisiert wird. Wenn eine Benachrichtigungsregel für die NT-Domänensynchronisierung aktiviert ist, wird bei jedem hinzugefügten oder entfernten System ein Ereignis generiert. (Diese Ereignisse werden im Audit-Protokoll angezeigt und können abgefragt werden.) Wenn Sie Agenten auf hinzugefügten Systemen ausbringen möchten, wird die Ausbringung für jedes hinzugefügte System ausgeführt. Nach Abschluss der Synchronisierung wird das Feld aktualisiert. Dabei wird die Uhrzeit und das Datum der letzten Synchronisierung und nicht der abgeschlossenen Agenten-Ausbringungen angezeigt. **Letzte Synchronisierung**

9 Klicken Sie zum manuellen Synchronisieren der Gruppe mit der Domäne auf **Vergleichen und aktualisieren**. Die Seite **Manuell vergleichen und aktualisieren** wird angezeigt.



Durch Klicken auf **Vergleichen und aktualisieren** werden alle Änderungen an den Synchronisierungseinstellungen gespeichert.

   a Wenn Sie über diese Seite Systeme aus der Gruppe entfernen, müssen Sie festlegen, ob deren Agenten beim Entfernen der Systeme ebenfalls entfernt werden sollen.

   b Wählen Sie nach Bedarf die Systeme aus, die Sie zur Gruppe hinzufügen bzw. daraus entfernen möchten. Klicken Sie dann auf **Gruppe aktualisieren**, um die ausgewählten Systeme hinzuzufügen. Die Seite **Synchronisierungseinstellungen für** wird angezeigt.

10 Klicken Sie auf **Speichern**, und zeigen Sie dann die Ergebnisse in der Systemstruktur an, wenn Sie auf **Jetzt synchronisieren** oder **Gruppe aktualisieren** geklickt haben.

Bringen Sie nach dem Hinzufügen der Systeme zur Systemstruktur Agenten auf ihnen aus, falls Sie nicht festgelegt haben, dass Agenten als Teil der Synchronisierung ausgebracht werden sollen. Außerdem kann es sinnvoll sein, einen regelmäßigen Server-Task "NT-Domänen-/Active Directory-Synchronisierung" einzurichten, damit diese Gruppe mit allen neuen Systemen in der NT-Domäne aktualisiert wird.

Planen der Systemstruktursynchronisierung

Sie können einen Server-Task planen, der die Systemstruktur mit Änderungen in der zugeordneten Domäne oder dem zugeordneten Active Directory-Container aktualisiert.

Je nach Synchronisierungseinstellungen der Gruppe wird Folgendes ausgeführt:

- Hinzufügen neuer Systeme zur angegebenen Gruppe im Netzwerk
- Hinzufügen neuer zugehöriger Gruppen, wenn neue Active Directory-Container erstellt werden
- Löschen zugehöriger Gruppen, wenn Active Directory-Container entfernt werden
- Ausbringen von Agenten auf neue Systeme
- Entfernen von Systemen, die sich nicht mehr in der Domäne oder im Container befinden
- Anwenden von Richtlinien und Tasks der Site oder Gruppe auf neue Systeme
- Verhindern oder Zulassen doppelter Systemeinträge, die noch in der Systemstruktur vorhanden sind, die Sie an andere Stellen verschoben haben



Der Agent kann nicht auf allen Betriebssystemen auf diese Weise ausgebracht werden. Möglicherweise müssen Sie den Agenten auf einigen Systemen manuell verteilen.

Vorgehensweise

Definitionen zu Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

1 Klicken Sie auf **Menü** | **Automatisierung** | **Server-Tasks**, und klicken Sie dann auf **Aktionen** | **Neuer Task**. Der **Generator für Server-Tasks** wird geöffnet.

2 Geben Sie auf der Seite **Beschreibung** einen Namen für den Task an, und legen Sie fest, ob er nach dem Erstellen aktiviert werden soll. Klicken Sie dann auf **Weiter**. Die Seite **Aktionen** wird angezeigt.

3 Wählen Sie in der Dropdown-Liste den Eintrag **Active Directory-Synchronisierung/NT-Domäne** aus.

4 Legen Sie fest, ob alle Gruppen oder nur ausgewählte Gruppen synchronisiert werden sollen. Wenn Sie nur einige synchronisierte Gruppen synchronisieren möchten, klicken Sie auf **Synchronisierte Gruppen auswählen**, und wählen Sie die gewünschten Gruppen aus.

5 Klicken Sie auf **Weiter**. Die Seite **Plan** wird angezeigt.

6 Planen Sie den Task, und klicken Sie dann auf **Weiter**. Die Seite **Zusammenfassung** wird angezeigt.

7 Überprüfen Sie die Task-Details, und klicken Sie dann auf **Speichern**.



Sie können den Task nicht nur zur geplanten Zeit ausführen, sondern auch sofort, indem Sie auf der Seite **Server-Tasks** neben dem Task auf **Ausführen** klicken.

Manuelles Aktualisieren einer synchronisierten Gruppe mit einer NT-Domäne

Aktualisieren Sie eine synchronisierte Gruppe mit Änderungen in der zugehörigen NT-Domäne.

Die Aktualisierung beinhaltet die folgenden Änderungen:

- Hinzufügen von Systemen, die aktuell in der Domäne vorhanden sind
- Entfernen von Systemen aus der Systemstruktur, die sich nicht mehr in der Domäne befinden
- Entfernen von Agenten aus allen Systemen, die nicht mehr zur angegebenen Domäne gehören

Vorgehensweise

Definitionen zu Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

1 Klicken Sie auf **Menü** | **Systeme** | **Systemstruktur** | **Gruppeninformationen**, und wählen Sie dann die Gruppe aus, die der NT-Domäne zugewiesen ist.

2 Klicken Sie neben **Synchronisierungstyp** auf **Bearbeiten**. Die Seite **Synchronisierungseinstellungen** wird angezeigt.

3 Wählen Sie **NT-Domäne** aus, und klicken Sie dann unten auf der Seite auf **Vergleichen und aktualisieren**. Die Seite **Manuell vergleichen und aktualisieren** wird angezeigt.

4 Legen Sie beim Entfernen von Systemen aus der Gruppe fest, ob die Agenten von entfernten Systemen ebenfalls entfernt werden sollen.

5 Klicken Sie auf **Alle hinzufügen** bzw. **Hinzufügen**, um Systeme aus der Netzwerkdomäne in die ausgewählte Gruppe zu importieren.

Klicken Sie auf **Alle entfernen** bzw. **Entfernen**, um Systeme aus der ausgewählten Gruppe zu entfernen.

6 Klicken Sie abschließend auf **Gruppe aktualisieren**.

Verschieben von Systemen innerhalb der Systemstruktur

Verschieben Sie Systeme aus einer Gruppe in der Systemstruktur in eine andere. Sie können Systeme von beliebigen Seiten verschieben, auf denen eine Tabelle mit Systemen (einschließlich der Ergebnisse einer Abfrage) angezeigt wird.



Zusätzlich zu den unten angegebenen Schritten können Sie Systeme auch aus der Tabelle **Systeme** in eine beliebige Systemstrukturgruppe ziehen und dort ablegen.

Selbst wenn Sie Ihre Systemstruktur so gut organisiert haben, dass sie Ihre Netzwerkhierarchie genau wiedergibt, und Sie die Systemstruktur regelmäßig mithilfe automatisierter Tasks und Tools synchronisieren, müssen Sie möglicherweise Systeme manuell zwischen Gruppen verschieben. Beispielsweise könnte es erforderlich sein, dass Sie Systeme in bestimmten Abständen aus der Sammelgruppe verschieben müssen.

Vorgehensweise

Definitionen zu Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

1. Klicken Sie auf **Menü** | **Systeme** | **Systemstruktur** | **Systeme**, suchen Sie die Systeme, und wählen Sie sie aus.
2. Klicken Sie auf **Aktionen** | **Verzeichnisverwaltung** | **Systeme verschieben**. Die Seite **Neue Gruppe auswählen** wird angezeigt.
3. Legen Sie fest, ob die Systemstruktursortierung auf den ausgewählten Systemen beim Verschieben aktiviert oder deaktiviert werden soll.
4. Wählen Sie die Gruppe aus, in die die Systeme eingeordnet werden sollen, und klicken Sie dann auf **OK**.

Übertragen von Systemen auf einen anderen Server

Bevor Sie Systeme auf einen anderen McAfee ePO-Server übertragen können, müssen Sie den ASSC-Schlüssel (Agent-Server Secure Communication) für die sichere Kommunikation zwischen Agent und Server konfigurieren.

Bevor Sie beginnen

Konfigurieren Sie die folgenden Anforderungen, bevor Sie Systeme zwischen McAfee ePO-Servern übertragen:

- Tauschen Sie den ASSC-Schlüssel zwischen den Servern aus.



Die folgenden Schritte bewirken eine bidirektionale Übertragung. Wenn Sie nur unidirektionale Übertragungen aktivieren möchten, müssen Sie den Schlüssel vom Ziel-Server nicht auf den Haupt-Server importieren.

1. Exportieren Sie den Schlüssel für die Agenten-Server-Kommunikation von beiden Servern.
2. Importieren Sie den ASSC-Schlüssel aus Server A auf Server B.
3. Importieren Sie den ASSC-Schlüssel aus Server B auf Server A.

- Registrieren Sie den Server, auf den das System übertragen werden soll.



Achten Sie dabei darauf, dass Sie im **Generator für registrierte Server** auf der Seite **Details** die Option **Systeme übertragen** aktivieren.

Definitionen zu Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

Vorgehensweise

1. Klicken Sie auf **Menü** | **Systeme** | **Systemstruktur**, und wählen Sie dann die Systeme aus, die übertragen werden sollen.
2. Klicken Sie auf **Aktionen** | **Agent** | **Systeme übertragen**. Das Dialogfeld **Systeme übertragen** wird angezeigt.
3. Wählen Sie den gewünschten Server im Dropdown-Menü aus, und klicken Sie dann auf **OK**.



Nachdem ein verwaltetes System zur Übertragung gekennzeichnet wurde, müssen zwei Agent-zu-Server-Kommunikationsvorgänge erfolgen, bevor das System in der Systemstruktur des Ziel-Servers angezeigt wird. Die Zeitdauer, bis diese beiden Kommunikationsvorgänge abgeschlossen sind, hängt von der Konfiguration ab. Das standardmäßige Agent-zu-Server-Kommunikationsintervall beträgt eine Stunde.

10 Agent-zu-Server-Kommunikation

Die Benutzeroberfläche von ePolicy Orchestrator umfasst Seiten, auf denen Sie McAfee Agent-Tasks und Richtlinien konfigurieren sowie Systemeigenschaften, Agenten-Eigenschaften und andere McAfee-Produktinformationen anzeigen können.

Inhalt

Funktionsweise der Agent-zu-Server-Kommunikation

Der Agent muss in regelmäßigen Abständen mit einem ePolicy Orchestrator-Server oder einer Agentensteuerung kommunizieren, um sicherzustellen, dass alle Einstellungen aktuell sind, um Ereignisse zu senden, usw.

Diese Kommunikationsvorgänge werden als *Agent-zu-Server-Kommunikation* bezeichnet. Bei jedem Kommunikationsvorgang erfasst der Agent seine aktuellen Systemeigenschaften sowie alle noch nicht gesendeten Ereignisse und sendet sie an den Server. Der Server wiederum sendet neue oder geänderte Richtlinien und Tasks sowie eine Repository-Liste (wenn sich diese seit der letzten Agent-zu-Server-Kommunikation geändert hat) an den Agenten. Der Agent erzwingt die neuen Richtlinien lokal auf dem verwalteten System und übernimmt alle Änderungen an Tasks oder Repositories.

Der ePolicy Orchestrator-Server verwendet ein branchenübliches, standardisiertes TLS-Netzwerkprotokoll (Transport Layer Security) für sichere Netzwerkübertragungen.

Nach seiner Erstinstallation meldet sich der Agent zu einem beliebigen, zufallsgenerierten Zeitpunkt innerhalb von sechs Sekunden beim Server. Danach meldet sich der Agent immer dann, wenn eine der folgenden Situationen eintritt:

- Wenn das Agent-zu-Server-Kommunikationsintervall (ASKI) abgelaufen ist.
- Wenn Agenten-Reaktivierungen von McAfee ePO oder von Agentensteuerungen gesendet werden.
- Wenn ein geplanter Reaktivierungs-Task auf den Client-Systemen ausgeführt wird.

- Wenn die Kommunikation auf dem verwalteten System manuell ausgelöst wird.
- Wenn Agenten-Reaktivierungen vom ePolicy Orchestrator-Server gesendet werden.

Agent-zu-Server-Kommunikationsintervall (ASKI)

Das Agent-zu-Server-Kommunikationsintervall (ASKI) bestimmt, wie oft sich der McAfee Agent beim McAfee ePO-Server zurückmeldet.

Das Agent-zu-Server-Kommunikationsintervall wird auf der McAfee Agent-Richtlinienseite auf der Registerkarte **Allgemein** eingestellt. Die Standardeinstellung von 60 Minuten bedeutet, dass der Agent den Server einmal pro Stunde kontaktiert. Wenn Sie über eine Intervalländerung nachdenken, sollten Sie beachten, dass der Agent in jedem ASKI die folgenden Aktionen durchführt:

- Er erfasst und sendet seine Eigenschaften.
- Er sendet Ereignisse von niedriger Priorität, die seit der letzten Agent-zu-Server-Kommunikation aufgetreten sind.
- Er erzwingt Richtlinien.
- Die Agentensteuerung oder der ePolicy Orchestrator-Server sendet neue Richtlinien und Tasks an den Client. Diese Aktion kann weitere ressourcenintensive Aktionen zur Folge haben.

Auch wenn diese Aktivitäten einen einzelnen Computer nicht allzu sehr belasten, kann eine Reihe von Faktoren dazu führen, dass die Lasten im Netzwerk, auf McAfee ePO-Servern oder in Agentensteuerungen deutlich ansteigen. Das wäre zum Beispiel unter den folgenden Umständen der Fall:

- Es gibt zahlreiche von ePolicy Orchestrator verwaltete Systeme.
- In Ihrer Organisation gibt es strenge Anforderungen zur Abwehr von Bedrohungen.
- Die Standorte im Netzwerk oder die physischen Standorte von Clients sind in Bezug auf Server oder Agentensteuerungen stark verteilt.
- Es ist nur eine unzureichende Bandbreite verfügbar.

Wenn diese Punkte auf Ihre Umgebung zutreffen, sollten Agent-zu-Server-Kommunikationen weniger häufig durchgeführt werden. Für Clients mit wichtigen Funktionen können Sie ein kürzeres Intervall festlegen.

Behandeln von Unterbrechungen bei der Agent-zu-Server-Kommunikation

Bei der Behandlung von Kommunikationsunterbrechungen werden Probleme behoben, die verhindern, dass ein System eine Verbindung zu einem McAfee ePO-Server herstellen kann.

Unterbrechungen der Kommunikation können aus vielerlei Gründen auftreten. Der Algorithmus für die Agent-zu-Server-Kommunikation ist so ausgelegt, dass ein erneuter Versuch durchgeführt wird, wenn der erste Verbindungsversuch fehlschlägt.

Der McAfee Agent durchläuft die folgenden Verbindungsmethoden bis zu sechs Mal oder so lange, bis eine Antwort aus einem Satz von Antworten zurückgegeben wird.

1. IP-Adresse
2. Vollqualifizierter Domänenname
3. NetBIOS

Der Agent wiederholt diese drei Verbindungsmethoden in der aufgeführten Reihenfolge bis zu sechs Mal, was insgesamt 18 Verbindungsversuche bedeutet. Zwischen den einzelnen Verbindungsversuchen gibt es keine Verzögerung. Der ganze Vorgang wird beendet, wenn ein Verbindungsversuch zu einem der folgenden Ergebnisse führt:

- Kein Fehler
- Download fehlgeschlagen
- Upload fehlgeschlagen
- Agent wird heruntergefahren
- Übertragung abgebrochen
- Server ist belegt (Status-Code vom McAfee ePO-Server)
- Upload erfolgreich (Status-Code vom McAfee ePO-Server)
- Agent benötigt neue Schlüssel
- Kein zu empfangendes Paket (Status-Code vom McAfee ePO-Server)
- Agent muss GUID neu generieren (Status-Code vom McAfee ePO-Server)

Bei anderen Ergebnissen – zum Beispiel Verbindung abgelehnt, Fehler beim Verbinden, Zeitüberschreitung bei Verbindung – oder anderen Fehlern versucht der Agent unverzüglich, eine Verbindung mithilfe der nächsten in der Liste aufgeführten Methode herzustellen, bis der nächste ASKI näherrückt.

Reaktivierungen und Reaktivierungs-Tasks

Eine McAfee Agent-Reaktivierung löst sofort eine Agent-zu-Server-Kommunikation aus und nicht erst nach Ablauf des aktuellen Agent-zu-Server-Kommunikationsintervalls.



Der Client-Task zur Agenten-Reaktivierung wird nur auf Windows-Plattformen unterstützt. Zum Reaktivieren von Agenten auf Unix- und Macintosh-basierten Systemen müssen Sie Systemstrukturaktionen verwenden.

Eine Reaktivierung kann auf zwei Arten ausgegeben werden:

- **Manuell auf dem Server** – Das ist die gebräuchlichste Methode. Erforderlich ist hierbei, dass der Kommunikationsport für Agenten-Reaktivierungen geöffnet ist.
- **Nach einem vom Administrator festgelegten Zeitplan** – Diese Methode ist nützlich, wenn die manuelle Agent-zu-Server-Kommunikation laut Richtlinie deaktiviert ist. Der Administrator kann einen Reaktivierungs-*Task* erstellen und ausbringen, der den Agenten reaktiviert und eine Agent-zu-Server-Kommunikation veranlasst.

Für die Ausgabe einer Agenten-Reaktivierung gibt es u. a. folgende Gründe:

- Sie haben an einer Richtlinie eine Änderung vorgenommen, die unverzüglich und nicht erst nach Ablauf des nächsten geplanten Agent-zu-Server-Kommunikationsintervalls erzwungen werden soll.
- Sie haben einen neuen Task erstellt, der sofort ausgeführt werden soll. **Client-Task jetzt ausführen** erstellt einen Task, weist ihn dann den angegebenen Client-Systemen zu und sendet Reaktivierungen.
- Von einer Abfrage wurde ein Bericht generiert, aus dem hervorgeht, dass ein Client nicht konform ist, und Sie möchten nun dessen Status im Rahmen einer Fehlerbehebung testen.

Wenn Sie einen bestimmten Agenten auf einem Windows-System in einen SuperAgent konvertiert haben, kann dieser Reaktivierungen an vorgesehene Übertragungssegmente im Netzwerk senden. Durch SuperAgents wird die Bandbreitenbelastung bei Agenten-Reaktivierungen verteilt.

Senden manueller Reaktivierungen an einzelne Systeme

Das manuelle Senden einer Agenten- oder SuperAgent-Reaktivierung an Systeme in der **Systemstruktur** ist nützlich, wenn Sie Richtlinien ändern und möchten, dass sich Agenten schon vor der nächsten Agent-zu-Server-Kommunikation melden, um die aktualisierten Informationen zu senden oder zu empfangen.

Vorgehensweise

Definitionen zu Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

1. Klicken Sie auf **Menü** | **Systeme** | **Systemstruktur**, und wählen Sie dann die Gruppe aus, in der sich die Zielsysteme befinden.
2. Wählen Sie in der Liste die Systeme aus, und klicken Sie dann auf **Aktionen** | **Agent** | **Agenten reaktivieren**.
3. Vergewissern Sie sich, dass die von Ihnen ausgewählten Systeme im Abschnitt **Zielsysteme** angezeigt werden.
4. Legen Sie neben **Reaktivierungstyp** fest, ob eine **Agenten-Reaktivierung** oder eine **SuperAgent-Reaktivierung** gesendet werden soll.
5. Übernehmen Sie den Standardwert (0 Minuten), oder geben Sie ein anderes Intervall für den **Zufallsgenerator** ein (0 – 60 Minuten). Beachten Sie dabei, wie viele Systeme die Reaktivierung sofort empfangen würden und wie viel Bandbreite verfügbar ist. Wenn Sie `0` eingeben, reagieren die Agenten sofort.
6. Damit bei dieser Reaktivierung inkrementelle Produkteigenschaften gesendet werden, müssen Sie die Option **Zusätzlich zu Systemeigenschaften vollständige Produkteigenschaften abrufen** deaktivieren. In der Standardeinstellung werden vollständige Produkteigenschaften gesendet.
7. Damit bei dieser Reaktivierung alle Richtlinien und Tasks aktualisiert werden, aktivieren Sie die Option **Vollständige Richtlinien- und Task-Aktualisierung erzwingen**.
8. Geben Sie bei **Anzahl der Versuche**, **Wiederholungsintervall** und **Abbrechen nach** eigene Werte für diese Reaktivierung ein, falls Sie die Standardeinstellungen nicht übernehmen möchten.
9. Wählen Sie aus, ob die Agenten-Reaktivierung über **Alle Agentensteuerungen** oder über die **Zuletzt verbundene Agentensteuerung** erfolgen soll.
10. Klicken Sie auf **OK**, um die Agenten- oder SuperAgent-Reaktivierung zu senden.

Senden manueller Reaktivierungen an eine Gruppe

Eine Agent- oder SuperAgent-Reaktivierung kann in einer einzigen Aufgabe an eine ganze **Systemstruktur**-Gruppe gesendet werden. Dies ist nützlich, wenn Sie Richtlinien geändert haben und möchten, dass sich Agenten schon vor der nächsten Agent-zu-Server-Kommunikation melden, um die aktualisierten Informationen zu senden oder zu empfangen.

Vorgehensweise

Definitionen zu Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

1. Klicken Sie auf **Menü** | **Systeme** | **Systemstruktur**.
2. Wählen Sie in der **Systemstruktur** die Zielgruppe aus, und klicken Sie dann auf die Registerkarte **Gruppeninformationen**.
3. Klicken Sie auf **Aktionen** | **Agenten reaktivieren**.
4. Vergewissern Sie sich, dass neben **Zielgruppe** die ausgewählte Gruppe angezeigt wird.

5. Wählen Sie aus, ob eine Agenten-Reaktivierung zu **Allen Systemen in dieser Gruppe** oder **Allen Systemen in dieser Gruppe und Untergruppen** gesendet werden soll.
6. Legen Sie neben **Typ** fest, ob eine **Agenten-Reaktivierung** oder eine **SuperAgent-Reaktivierung** gesendet werden soll.
7. Übernehmen Sie den Standardwert (0 Minuten), oder geben Sie ein anderes Intervall für den **Zufallsgenerator** ein (0 – 60 Minuten). Wenn Sie `0` eingeben, reagieren die Agenten sofort.
8. Damit bei dieser Reaktivierung minimale Produkteigenschaften gesendet werden, deaktivieren Sie die Option **Zusätzlich zu Systemeigenschaften vollständige Produkteigenschaften abrufen**. In der Standardeinstellung werden vollständige Produkteigenschaften gesendet.
9. Damit bei dieser Reaktivierung alle Richtlinien und Tasks aktualisiert werden, aktivieren Sie die Option **Vollständige Richtlinien- und Task-Aktualisierung erzwingen**.
10. Klicken Sie auf **OK**, um die Agenten- oder SuperAgent-Reaktivierung zu senden.

Beschreibung und Funktionsweise von SuperAgents

Ein SuperAgent ist ein Agent, der als Mittler zwischen dem McAfee ePO-Server und anderen Agenten dient, die sich im gleichen Übertragungssegment des Netzwerks befinden. Nur ein Windows-Agent kann in einen SuperAgent umgewandelt werden.

Der SuperAgent legt Informationen im Cache ab, die er von einem ePolicy Orchestrator-Server, aus dem Master-Repository oder aus einem gespiegelten verteilten Repository empfängt, und verteilt diese an die Agenten in seinem Netzwerksubnetz. Die Funktion für verzögertes Caching ermöglicht es SuperAgents, Daten vom ePolicy Orchestrator-Server nur auf Anforderung von einem lokalen Agenten-Knoten abzurufen. Durch das Erstellen einer Hierarchie von SuperAgents und das Aktivieren von verzögertem Caching lässt sich noch mehr Bandbreite einsparen und der WAN-Datenverkehr minimieren.

Ein SuperAgent sendet auch Reaktivierungen an andere Agenten, die sich im gleichen Netzwerksubnetz befinden. Der SuperAgent empfängt eine Reaktivierung vom ePolicy Orchestrator-Server und reaktiviert dann die Agenten in seinem Subnetz.



Dies ist eine Alternative zum Versand gewöhnlicher Agenten-Reaktivierungen an jeden Agenten im Netzwerk oder zum Versand von Agenten-Reaktivierungs-Tasks an jeden Computer.

SuperAgents und Reaktivierungen

Wenn Sie Agent-zu-Server-Kommunikationen mithilfe von Agenten-Reaktivierungen initiieren möchten, sollten Sie in jedem Übertragungssegment des Netzwerks einen Agenten in einen SuperAgent umwandeln.

Durch SuperAgents wird die Bandbreitenbelastung bei gleichzeitig ausgeführten Reaktivierungen verteilt. Anstatt Agenten-Reaktivierungen vom Server an jeden Agenten zu senden, sendet der Server die SuperAgent-Reaktivierung an SuperAgents im ausgewählten Systemstruktursegment.

Der Prozess läuft folgendermaßen ab:

1. Der Server sendet die Reaktivierung an alle SuperAgents.
2. Die SuperAgents senden eine Reaktivierung an alle Agenten im selben Übertragungssegment.
3. Alle benachrichtigten Agenten (normale, von einem SuperAgent benachrichtigte Agenten sowie alle SuperAgents) tauschen Daten mit dem ePolicy Orchestrator-Server oder der Agentensteuerung aus.

Wenn eine SuperAgent-Reaktivierung gesendet wird, werden Agenten, in deren Übertragungssegment sich kein aktiver SuperAgent befindet, auch nicht aufgefordert, mit dem Server zu kommunizieren.

Tipps für die Ausbringung von SuperAgents

Um genügend SuperAgents an den richtigen Stellen auszubringen, bestimmen Sie zunächst die Übertragungssegmente in Ihrer Umgebung. Wählen Sie anschließend in jedem Segment ein System (vorzugsweise einen Server) aus, das als SuperAgent-Host dienen soll. Wenn Sie SuperAgents verwenden, müssen Sie sicherstellen, dass allen Agenten ein SuperAgent zugewiesen ist.

Agenten- und SuperAgent-Reaktivierungen nutzen dieselben sicheren Kanäle. Vergewissern Sie sich, dass die folgenden Ports nicht von einer Firewall auf dem Client blockiert werden:

- Der Kommunikationsport für Agenten-Reaktivierung (standardmäßig Port 8081)
- Der Kommunikationsport für Agenten-Übertragung (standardmäßig Port 8082)

Konvertieren von Agenten in SuperAgents

Wenn der SuperAgent während der globalen Aktualisierung eine Aktualisierung vom ePolicy Orchestrator-Server erhält, sendet er an alle Agenten in seinem Netzwerk Reaktivierungen. Um einen Agenten in einen SuperAgent umzuwandeln, müssen Sie SuperAgent-Richtlinieneinstellungen konfigurieren.

Vorgehensweise

Definitionen zu Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

1. Klicken Sie auf **Menü** | **Systeme** | **Systemstruktur** | **Systeme**, und wählen Sie dann in der Systemstruktur eine Gruppe aus. Alle Systeme aus dieser Gruppe werden im Detailbereich angezeigt.
2. Wählen Sie ein System aus, und klicken Sie auf **Aktionen** | **Agent** | **Richtlinien auf einem einzelnen System ändern**. Die Seite **Richtlinienzuweisung** für dieses System wird angezeigt.
3. Wählen Sie in der Dropdown-Liste **Produkt** den Eintrag **McAfee Agent** aus. Die Richtlinienkategorien unter **McAfee Agent** werden mit der dem System zugewiesenen Richtlinie aufgeführt.
4. Wenn die Richtlinie geerbt wurde, aktivieren Sie die Option **Vererbung unterbrechen und ab hier Richtlinie und Einstellungen zuweisen**.
5. Wählen Sie in der Dropdown-Liste **Zugewiesene Richtlinie** die gewünschte allgemeine Richtlinie aus.

   
   An dieser Stelle können Sie auch die ausgewählte Richtlinie bearbeiten oder eine neue Richtlinie erstellen.

6. Legen Sie fest, ob die Richtlinienvererbung gesperrt werden soll, um zu verhindern, dass Systemen, die diese Richtlinie erben, eine andere Richtlinie zugewiesen wird.
7. Wählen Sie auf der Registerkarte **SuperAgent** die Option **Agenten in SuperAgents konvertieren** aus, um die Übertragung von Reaktivierungen zu ermöglichen.
8. Klicken Sie auf **Speichern**.
9. Senden Sie eine Agenten-Reaktivierung.

Caching und Kommunikationsunterbrechungen bei SuperAgents

Der SuperAgent legt die Inhalte seines Repositorys auf eine bestimmte Weise im Cache ab, um die Belegung von WAN-Bandbreite zu minimieren.

Wenn ein Agent in einen SuperAgent umgewandelt wurde, kann er vom McAfee ePO-Server, von verteilten Repositories oder von anderen SuperAgents bezogene Inhalte im Cache ablegen, um sie lokal an andere Agenten zu verteilen, wodurch sich die Belegung von WAN-Bandbreite verringert. Um dieses Verhalten zu aktivieren, klicken Sie auf der Richtlinienseite **McAfee Agent | SuperAgent**, die Sie über **Menü | Richtlinie | Richtlinienkatalog** erreichen, auf **Verzögertes Caching aktivieren**.



Inhalte aus McAfee-HTTP- oder -FTP-Repositories können von den SuperAgents nicht im Cache abgelegt werden.

Funktionsweise des Caches

Wenn ein Client-System Inhalte erstmalig anfordert, werden diese Inhalte von dem diesem System zugewiesenen SuperAgent im Cache abgelegt. Von da an wird der Cache immer dann aktualisiert, wenn im Master-Repository eine neuere Version des angeforderten Pakets verfügbar ist. In einer hierarchischen Struktur von SuperAgents erhält ein untergeordneter SuperAgent die angeforderten Inhaltsaktualisierungen aus dem Cache des ihm übergeordneten SuperAgents.

Vom SuperAgent werden definitiv nur solche Inhalte zwischengespeichert, die von den ihm zugewiesenen Agenten benötigt werden, da er Inhalte immer erst dann aus den Repositories abruft, wenn sie von einem Client angefordert werden. Dadurch wird der Datenverkehr zwischen dem SuperAgent und den Repositories minimiert. Während der SuperAgent Inhalte aus dem Repository abruft, werden Anforderungen von Client-Systemen für diese Inhalte angehalten.



Der SuperAgent muss über Zugriff auf das Repository verfügen. Ohne diesen Zugriff würden Agenten, die Aktualisierungen vom SuperAgent beziehen, neue Inhalte nie erhalten. Stellen Sie sicher, dass die SuperAgent-Richtlinie einen Zugriff auf das Repository enthält.

Agenten, die so konfiguriert sind, dass sie den SuperAgent als ihr Repository verwenden, erhalten die Inhalte aus dem Cache des SuperAgent anstatt direkt vom McAfee ePO-Server. Dies verbessert die Leistung des Agenten-Systems, da der überwiegende Teil des Netzwerkverkehrs für den SuperAgent und dessen Clients lokal erfolgt.

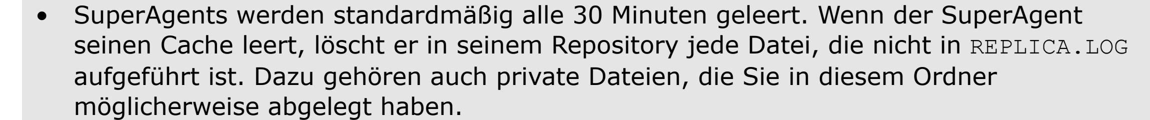
Wenn der SuperAgent so umkonfiguriert wird, dass er ein neues Repository verwendet, wird der Cache in Bezug auf das neue Repository aktualisiert.

Wann wird der Cache geleert?

SuperAgents leeren unter zwei Umständen die Inhalte Ihres Caches:

- Wenn das **Intervall zum Überprüfen der Repositories auf neuen Inhalt** seit der letzten Anforderung von Aktualisierungen abgelaufen ist, lädt der SuperAgent Aktualisierungen aus dem Master-Repository herunter, verarbeitet sie und leert den Cache vollständig, wenn neue Inhalte verfügbar sind.
- Bei einer globalen Aktualisierung erhalten die SuperAgents eine Reaktivierung, die sämtliche Inhalte aus dem Cache leert.





- SuperAgents werden standardmäßig alle 30 Minuten geleert. Wenn der SuperAgent seinen Cache leert, löscht er in seinem Repository jede Datei, die nicht in `REPLICA.LOG` aufgeführt ist. Dazu gehören auch private Dateien, die Sie in diesem Ordner möglicherweise abgelegt haben.
- Das SuperAgent-Caching sollte nicht zusammen mit Repository-Replizierungen verwendet werden.

Umgang mit Kommunikationsunterbrechungen

Wenn ein SuperAgent eine Anforderung von Inhalten empfängt, die möglicherweise veraltet sind, kontaktiert er den McAfee ePO-Server, um zu ermitteln, ob neue Inhalte verfügbar sind. Wenn es bei den Verbindungsversuchen zu einer Zeitüberschreitung kommt, verteilt der SuperAgent die Inhalte stattdessen aus seinem eigenen Repository. Dadurch soll sichergestellt werden, dass die anfordernde Seite Inhalte erhält, selbst wenn diese möglicherweise veraltet sind.



Das SuperAgent-Caching sollte nicht zusammen mit globalen Aktualisierungen verwendet werden. Beide erfüllen in einer verwalteten Umgebung die gleiche Funktion – sie halten die verteilten Repositories auf dem aktuellen Stand. Sie ergänzen sich jedoch nicht gegenseitig. Setzen Sie SuperAgent-Caching ein, wenn vor allem die Bandbreitenauslastung begrenzt werden soll. Globale Aktualisierung können Sie verwenden, wenn besonders Wert auf schnelle Aktualisierungen im Unternehmen gelegt wird.

SuperAgents und deren Hierarchie

Eine Hierarchie von SuperAgents kann Agenten, die sich im gleichen Netzwerk befinden, bei einer Minimierung der Netzwerkauslastung helfen.

Ein SuperAgent speichert die Inhaltsaktualisierungen aus dem ePolicy Orchestrator-Server oder aus dem verteilten Repository im Cache und gibt sie an Agenten im Netzwerk weiter, wodurch weniger WAN-Datenverkehr anfällt. Im Idealfall sollten mehrere SuperAgents vorhanden sein, um die Netzwerklast optimal zu verteilen.



Vor dem Einrichten der SuperAgent-Hierarchie müssen Sie sich vergewissern, dass das verzögerte Caching aktiviert ist.

Anordnen von SuperAgents in einer Hierarchie

Allgemeine und Repository-Richtlinien können so geändert werden, dass eine SuperAgent-Hierarchie aktiviert und festgelegt werden kann.

Vorgehensweise

Definitionen zu Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

1. Klicken Sie auf **Menü** | **Richtlinie** | **Richtlinienkatalog**, und wählen Sie dann im Dropdown-Menü **Produkt** den Eintrag **McAfee Agent** sowie im Dropdown-Menü **Kategorie** den Eintrag **Allgemein** aus.
2. Klicken Sie auf die Richtlinie **My Default**, um die Richtlinie zu bearbeiten. Wenn Sie eine Richtlinie erstellen möchten, klicken Sie auf **Aktionen** | **Neue Richtlinie**.

   Die Richtlinie **McAfee Default** kann nicht geändert werden.
3. Wählen Sie auf der Registerkarte **SuperAgent** die Option **Agenten in SuperAgents konvertieren** aus, um den Agenten in einen SuperAgent umzuwandeln und sein Repository mit den neuesten Inhalten zu aktualisieren.
4. Wählen Sie **Systeme mit SuperAgents als verteilte Repositories verwenden** aus, um die Systeme, auf denen sich SuperAgents befinden, als Aktualisierungs-Repositories für die Systeme in deren Übertragungssegment zu verwenden. Geben Sie dann den **Repository-Pfad** an.
5. Wählen Sie **Verzögertes Caching aktivieren** aus, damit SuperAgents die vom McAfee ePO-Server empfangenen Inhalte im Cache ablegen können.
6. Klicken Sie auf **Speichern**.

   Auf der Seite **Richtlinienkatalog** werden die Richtlinien vom Typ **Allgemein** aufgeführt.

7 Ändern Sie die **Kategorie** zu **Repository**, und klicken Sie dann auf die Richtlinie **My Default**, um mit dem Bearbeiten der Richtlinie zu beginnen. Wenn Sie eine Richtlinie erstellen möchten, klicken Sie auf **Aktionen | Neue Richtlinie**.

8 Aktivieren Sie auf der Registerkarte **Repositories** die Option **Reihenfolge in der Repository-Liste verwenden**.

9 Klicken Sie auf **Zugriff von Clients auf neu hinzugefügte Repositories automatisch zulassen**, um neue SuperAgent-Repositories zur Liste hinzuzufügen. Klicken Sie dann auf **Zum Anfang**, um die SuperAgents hierarchisch anzuordnen.



Sortieren Sie die Repositories so, dass der übergeordnete SuperAgent immer ganz oben in der Repository-Liste steht.

10 Klicken Sie auf **Speichern**.

Nach dem Festlegen der SuperAgent-Hierarchie können Sie den Task **McAfee Agent-Statistik** erstellen und ausführen, um einen Bericht über die Einsparungen bei der Netzwerkbandbreite zu erstellen. Weitere Einzelheiten dazu finden Sie unter *Erfassen von McAfee Agent-Statistiken*.

Erstellen einer Hierarchie von SuperAgents

Sie können die Hierarchie mithilfe der Repository-Richtlinie erstellen. Es wird empfohlen, dass Sie im Netzwerk eine dreistufige Hierarchie von SuperAgents pflegen.

Durch eine Hierarchie von SuperAgents wird verhindert, dass identische Inhaltsaktualisierungen mehrmals vom ePolicy Orchestrator-Server oder aus dem verteilten Repository heruntergeladen werden. In einem Client-Netzwerk mit zwei SuperAgents (SuperAgent 1 und SuperAgent 2) sowie einem verteilten Repository können Sie die Hierarchie beispielsweise so konfigurieren, dass die Client-Systeme ihre Inhaltsaktualisierungen vom SuperAgent 1 erhalten. Der SuperAgent 1 empfängt seine Aktualisierungen vom SuperAgent 2 und legt diese im Cache ab. Der SuperAgent 2 wiederum erhält seine Aktualisierungen aus dem verteilten Repository und legt diese im Cache ab.



Inhalte aus McAfee-HTTP- oder -FTP-Repositories können von den SuperAgents nicht im Cache abgelegt werden.

Beim Erstellen einer Hierarchie müssen Sie darauf achten, dass die Hierarchie keinen Kreis bildet. Ein solcher Kreis würde zum Beispiel gebildet, wenn SuperAgent 1 so konfiguriert ist, dass er Aktualisierungen vom SuperAgent 2 abruft, SuperAgent 2 so konfiguriert ist, dass er Aktualisierungen vom SuperAgent 3 abruft, und SuperAgent 3 wiederum so konfiguriert ist, dass er Aktualisierungen vom SuperAgent 1 abruft.

Damit sichergestellt ist, dass der übergeordnete SuperAgent immer über die neuesten Inhaltsaktualisierungen verfügt, muss die Übertragung von SuperAgent-Reaktivierungen aktiviert sein. Weitere Informationen dazu finden Sie unter *Aktivieren der Übertragung von SuperAgent-Reaktivierungen*.



Wenn die SuperAgents die Agenten nicht mit den aktuellsten Inhaltsaktualisierungen versorgen, lehnen die Agenten die vom SuperAgent erhaltene Aktualisierung ab und weichen auf das nächste in der Richtlinie konfigurierte Repository aus.

Relay-Funktionalität des Agenten

Wenn die Kommunikation zwischen McAfee Agent und dem McAfee ePO-Server durch eine Netzwerkkonfiguration blockiert wird, kann der Agent keine Richtlinien und Aktualisierungen von Inhalten empfangen oder Ereignisse senden.

Zur Überbrückung der Kommunikation zwischen den Client-Systemen und dem McAfee ePO-Server kann bei Agenten, die über eine direkte Verbindung zum ePolicy Orchestrator-Server oder zu Agentensteuerungen verfügen, die Relay-Funktionalität aktiviert werden. Sie können auch mehrere Agenten als Relay-Server konfigurieren, um die Netzwerklast gleichmäßiger zu verteilen.



- McAfee Agent verfügt ab der Version 4.8 über Relay-Funktionalität.
- Der ePolicy Orchestrator-Server kann eine Kommunikation (z. B. das Anzeigen von Agenten-Protokollen) nur mit einem direkt verbundenen Agenten initiieren.
- Auf AIX-Systemen wird die Relay-Funktionalität nicht unterstützt.

Kommunikation über Relay-Server

Durch Aktivieren der Relay-Funktionalität im Netzwerk wird ein Agent in einen Relay-Server umgewandelt. Agenten mit Relay-Funktion können auf den ePolicy Orchestrator-Server oder auf das verteilte Repository zugreifen.

Wenn ein Agent keine direkte Verbindung zum ePolicy Orchestrator-Server oder zur Agentensteuerung herstellen kann, sendet er eine Nachricht, um in seinem Netzwerk einen Agenten mit Relay-Funktionalität zu finden. Die Relay-Server antworten auf die Nachricht, und der Agent stellt eine Verbindung zu dem Server her, der als erster geantwortet hat.

Wenn ein Agent keine direkte Verbindung zum ePolicy Orchestrator-Server oder zur Agentensteuerung herstellen kann, versucht er, eine Verbindung zum ersten Relay-Server aufzubauen, der auf seine Suchnachricht geantwortet hat. Der Agent ermittelt in jedem Agent-zu-Server-Kommunikationsintervall (ASKI) die Relay-Server im Netzwerk und legt die Details zu den ersten fünf Relay-Servern im Cache ab, die auf die Suchnachricht geantwortet haben. Wenn der aktuelle Relay-Server keine Verbindung zum ePolicy Orchestrator-Server herstellen kann oder nicht über die benötigte Inhaltsaktualisierung verfügt, stellt der Agent eine Verbindung zum nächsten Relay-Server aus seinem Cache her.



- Zum Auffinden der Relay-Server im Netzwerk müssen Agenten über das UDP-Protokoll (User Datagram Protocol) verfügen.
- Relay-Server stellen nur Verbindungen zu dem ePolicy Orchestrator-Server oder den verteilten Repositories her, die in ihrer Datei `SITELIST.XML` aufgeführt sind. McAfee empfiehlt, die Datei `SITELIST.XML` des Relay-Servers als Obermenge der Sitelists aller Agenten aufzunehmen, die für Verbindungen über dieses Relay konfiguriert sind.

Auf Windows-Client-Systemen wird nach dem Aktivieren der Relay-Funktionalität über die Richtlinie ein neuer Dienst **MFESERVICEMGR.EXE** installiert. Durch Starten und Beenden dieses Diensts kann die Relay-Funktionalität auf dem Client-System gesteuert werden.

Nachdem der Agent alle gewünschten Inhalte vom ePolicy Orchestrator-Server hoch- oder heruntergeladen hat, trennt der Relay-Server die Verbindung zum Agenten und zum ePolicy Orchestrator-Server.

Aktivieren der Relay-Funktionalität

Zum Aktivieren der Relay-Funktionalität in einem Agenten können Sie Richtlinien konfigurieren und zuweisen.



Wenn Sie ein System mit einem anderen Betriebssystem als Windows als Relay-Server aktivieren, müssen Sie darauf achten, dass Sie manuell eine Ausnahme für den Prozess `cmamesh` und den Service-Manager-Port in den `iptables` und `ip6tables` hinzufügen.

Vorgehensweise

Definitionen zu Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

1. Klicken Sie auf **Menü** | **Systeme** | **Systemstruktur** | **Systeme**, und wählen Sie dann in der Systemstruktur eine Gruppe aus. Alle Systeme aus dieser Gruppe werden im Detailbereich angezeigt.
2. Wählen Sie ein System aus, und klicken Sie auf **Aktionen** | **Agent** | **Richtlinien auf einem einzelnen System ändern**. Die Seite **Richtlinienzuweisung** für dieses System wird angezeigt.
3. Wählen Sie in der Dropdown-Liste **Produkt** den Eintrag **McAfee Agent** aus. Die Richtlinienkategorien unter **McAfee Agent** werden mit der dem System zugewiesenen Richtlinie aufgeführt.
4. Wenn die Richtlinie geerbt wurde, aktivieren Sie die Option **Vererbung unterbrechen und ab hier Richtlinie und Einstellungen zuweisen**.
5. Wählen Sie in der Dropdown-Liste **Zugewiesene Richtlinie** die gewünschte allgemeine Richtlinie aus.

   An dieser Stelle können Sie auch die ausgewählte Richtlinie bearbeiten oder eine neue Richtlinie erstellen.

6. Legen Sie fest, ob die Richtlinienvererbung gesperrt werden soll, um zu verhindern, dass Systemen, die diese Richtlinie erben, eine andere Richtlinie zugewiesen wird.
7. Wählen Sie auf der Registerkarte **SuperAgent** die Option **Relay-Dienst aktivieren** aus, um die Relay-Funktionalität zu aktivieren.

   - Vergewissern Sie sich, dass der **Service-Manager-Port** auf **8083** eingestellt ist.
   - McAfee empfiehlt, die Relay-Funktionalität im Netzwerk Ihrer Organisation zu aktivieren.
   - Relay-Server können über Proxy-Einstellungen keine Verbindungen zu den ePolicy Orchestrator-Servern herstellen.

8. Klicken Sie auf **Speichern**.
9. Senden Sie eine Agenten-Reaktivierung.

   - Nach dem ersten ASKI ist der Status des Relay-Diensts auf der Seite **McAfee Agent-Eigenschaften** oder in der McTray-Benutzeroberfläche auf dem Client-System aktualisiert.
   - Auf Windows-Client-Systemen wird die Protokolldatei `SVCMGR_<Systemname>.LOG` unter `C:\ProgramData\McAfee\Common Framework\DB` gespeichert.

Erfassen von McAfee Agent-Statistiken

Sie können den Client-Task "McAfee Agent-Statistik" auf den verwalteten Knoten ausführen, um statistische Angaben über den Relay-Server und die SuperAgent-Hierarchie zu erfassen.

Vorgehensweise

Definitionen zu Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

1. Klicken Sie auf **Menü** | **Systeme** | **Systemstruktur** | **Systeme**, und wählen Sie dann in der Systemstruktur eine Gruppe aus. Alle Systeme aus dieser Gruppe werden im Detailbereich angezeigt.
2. Wählen Sie ein System aus, und klicken Sie auf **Aktionen** | **Agent** | **Tasks auf einem einzelnen System ändern**. Die diesem System zugewiesenen Client-Tasks werden angezeigt.
3. Klicken Sie auf **Aktionen** | **Neue Client-Task-Zuweisung**. Die Seite **Generator für Client-Task-Zuweisungen** wird angezeigt.
4. Wählen Sie in der Liste **Produkt** den Eintrag **McAfee Agent** und bei **Task-Typ** den Eintrag **McAfee Agent-Statistik** aus.
5. Klicken Sie auf **Neuen Task erstellen**. Die Seite **Neuer Client-Task** wird angezeigt.
6. Wählen Sie die gewünschte Option aus, und klicken Sie dann auf **Speichern**.

Option	Definition
Relay-Server-Statistiken	Erfasst die folgenden Statistiken auf den Client-Systemen: • Die Anzahl der fehlgeschlagenen Verbindungen von Relay-Servern zum ePolicy Orchestrator-Server oder zu den verteilten Repositories. • Die Anzahl der Verbindungen, die vom Relay-Server abgelehnt wurden, nachdem die maximale Anzahl an Verbindungen hergestellt wurde.
Statistiken der hierarchischen SuperAgent-Aktualisierung	Erfasst die durch Verwendung der SuperAgent-Hierarchie eingesparte Netzwerkbandbreite.



Sobald der Task auf dem Client-System ausgebracht und der Status an ePolicy Orchestrator gemeldet wurde, wird die Statistik auf 0 zurückgesetzt.

Deaktivieren der Relay-Funktionalität

Sie können die Richtlinie **Allgemein** verwenden, um die Relay-Dienste auf dem Agenten zu deaktivieren.

Definitionen zu Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

Vorgehensweise

1. Klicken Sie auf **Menü** | **Systeme** | **Systemstruktur** | **Systeme**, und wählen Sie dann in der Systemstruktur eine Gruppe aus. Alle Systeme aus dieser Gruppe werden im Detailbereich angezeigt.
2. Wählen Sie das System aus, auf dem die Relay-Funktionalität aktiviert war, und klicken Sie dann auf **Aktionen** | **Agent** | **Richtlinien auf einem einzelnen System ändern**. Die Seite **Richtlinienzuweisung** für dieses System wird angezeigt.
3. Wählen Sie in der Dropdown-Liste **Produkt** den Eintrag **McAfee Agent** aus. Die Richtlinienkategorien unter **McAfee Agent** werden mit der dem System zugewiesenen Richtlinie aufgeführt.
4. Wählen Sie in der Dropdown-Liste **Zugewiesene Richtlinie** die Richtlinie **Allgemein** aus, die auf dem Client-System erzwungen wird.
5. Deaktivieren Sie auf der Registerkarte **SuperAgent** die Option **Relay-Dienst aktivieren**, um die Relay-Funktionalität auf dem Client-System zu deaktivieren.

6 Klicken Sie auf **Speichern**.

7 Senden Sie eine Agenten-Reaktivierung.

Antworten auf Richtlinienereignisse

Sie können eine automatische Antwort in ePolicy Orchestrator einrichten, die so gefiltert wird, dass nur Richtlinienereignisse angezeigt werden.

Vorgehensweise

Definitionen zu Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

1. Klicken Sie auf **Menü** | **Automatisierung** | **Automatische Antworten**, um die Seite **Automatische Antworten** zu öffnen.
2. Klicken Sie auf **Aktionen** | **Neue Antwort**.
3. Geben Sie einen **Namen** für die Antwort und eine optionale **Beschreibung** ein.
4. Wählen Sie bei der **Ereignisgruppe** den Eintrag **ePO-Benachrichtigungsereignisse** und beim **Ereignistyp** den Eintrag **Client**, **Bedrohung** oder **Server** aus.
5. Klicken Sie auf **Aktiviert**, um die Antwort zu aktivieren, und klicken Sie dann auf **Weiter**.
6. Wählen Sie in **Verfügbare Eigenschaften** den Eintrag **Ereignisbeschreibung** aus.
7. Klicken Sie in der Zeile **Ereignisbeschreibung** auf die Schaltfläche zum Durchsuchen [...], und wählen Sie eine der folgenden Optionen in der Liste aus:

Option	Definition
Fehler beim Erfassen von Eigenschaften für Einzelprodukte durch Agenten	Dieses Ereignis wird generiert und weitergeleitet, wenn zum ersten Mal ein Fehler bei der Erfassung von Eigenschaften auftritt. Ein nachfolgendes Ereignis vom Typ "Erfolg" wird nicht generiert. Jeder Fehler bei einem Einzelprodukt generiert ein eigenes Ereignis.
Fehler beim Erzwingen der Richtlinie für Einzelprodukte durch Agenten	Dieses Ereignis wird generiert und weitergeleitet, wenn zum ersten Mal ein Fehler bei der Richtlinienerzwingung auftritt. Ein nachfolgendes Ereignis vom Typ "Erfolg" wird nicht generiert. Jeder Fehler bei einem Einzelprodukt generiert ein eigenes Ereignis.

8. Geben Sie gegebenenfalls die restlichen Informationen in den Filter ein, und klicken Sie dann auf **Weiter**.
9. Wählen Sie die Optionen **Aggregation**, **Gruppierung** und **Beschränkung** je nach Bedarf aus.
10. Wählen Sie einen Aktionstyp aus, geben Sie das gewünschte Verhalten je nach Aktionstyp ein, und klicken Sie dann auf **Weiter**.
11. Überprüfen Sie die Zusammenfassung des Antwortverhaltens. Wenn alles korrekt ist, klicken Sie auf **Speichern**.

Es wurde nun eine automatische Antwort erstellt, die beim Eintreten eines Richtlinienereignisses die beschriebene Aktion ausführt.

Sofortiges Ausführen von Client-Tasks

Wenn ePolicy Orchestrator 4.6 (und höher) mit McAfee Agent 4.6 (und höher) kommuniziert, können Sie Client-Tasks mithilfe der Funktion **Task jetzt ausführen** sofort ausführen.

Anstatt Tasks nach ihrer Planung sofort auszuführen, reiht McAfee Agent sie in einer Warteschlange ein. Während dieses Platzieren in einer Warteschlange sofort erfolgt, wird mit der Ausführung eines Tasks nur dann auch begonnen, wenn sich in der Warteschlange keine weiteren Tasks vor ihm befinden. Im Rahmen der Vorgehensweise **Client-Task jetzt ausführen** erstellte Tasks werden ausgeführt, und der Task wird nach Abschluss auf dem Client gelöscht.



Die Funktion **Client-Task jetzt ausführen** wird nur auf Client-Systemen mit Windows unterstützt.

Vorgehensweise

Definitionen zu Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

1. Klicken Sie auf **Menü** | **Systeme** | **Systemstruktur**.
2. Wählen Sie ein oder mehrere Systeme aus, auf denen ein Task ausgeführt werden soll.
3. Klicken Sie auf **Aktionen** | **Agent** | **Client-Task jetzt ausführen**.
4. Wählen Sie bei **Produkt** den Eintrag **McAfee Agent** sowie den **Task-Typ** aus.
5. Zum Ausführen eines vorhandenen Tasks klicken Sie auf den entsprechenden **Task-Namen** und dann auf **Task jetzt ausführen**.
6. Zum Definieren eines neues Tasks klicken Sie auf **Neuen Task erstellen**.
   a. Geben Sie die entsprechenden Informationen zu dem Task ein, den Sie erstellen.

   Wenn Sie bei dieser Vorgehensweise einen **McAfee Agent Produktausbringungs**- oder **Produktaktualisierungs**-Task erstellen, ist die Option **Bei jeder Richtlinienerzwingung ausführen** verfügbar. Diese Option hat keine Auswirkungen, da der Task nach seinem Abschluss gelöscht wird.

Die Seite **Client-Task-Ausführungsstatus** wird angezeigt, die den Status aller ausgeführten Tasks enthält. Wenn die Tasks abgeschlossen sind, können die Ergebnisse im Audit-Protokoll und im Server-Task-Protokoll angezeigt werden.

Ermitteln inaktiver Agenten

Ein inaktiver Agent ist ein Agent, der innerhalb eines vom Benutzer angegebenen Zeitraums nicht mit dem McAfee ePO-Server kommuniziert hat.

Einige Agenten können von Endbenutzern deaktiviert oder deinstalliert werden. Es kann auch vorkommen, dass das System, auf dem der Agent installiert wurde, aus dem Netzwerk entfernt wird. Sie sollten regelmäßig (wöchentlich) nach Systemen mit inaktiven Agenten suchen.

Vorgehensweise

Definitionen zu Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

1. Klicken Sie auf **Menü** | **Berichterstellung** | **Abfragen und Berichte**.
2. Wählen Sie in der Liste **Gruppen** die freigegebene Gruppe **McAfee Agent** aus.
3. Klicken Sie in der Zeile **Inaktive Agenten** auf **Ausführen**, um die Abfrage auszuführen.

   In der Standardkonfiguration sucht diese Abfrage Systeme, die im letzten Monat nicht mit dem McAfee ePO-Server kommuniziert haben. Sie können Stunden, Tage, Wochen, Quartale oder Jahre angeben.

Wenn Sie inaktive Agenten finden, überprüfen Sie deren Aktivitätsprotokolle auf Probleme, die die Ursache für die gestörte Agent-zu-Server-Kommunikation sein könnten. Mithilfe der Abfragergebnisse können Sie verschiedene Aktionen an den ermittelten Systemen durchführen (z. B. Senden eines Ping-Befehls an einen Agenten, Löschen, Reaktivieren und erneutes Ausbringen eines Agenten).

Windows-Systeme und vom Agenten gemeldete Produkteigenschaften

Der Agent meldet Systemeigenschaften aus den von ihm verwalteten Systemen an ePolicy Orchestrator. Welche Eigenschaften gemeldet werden, variiert je nach Betriebssystem. Bei den aufgeführten Eigenschaften handelt es sich um Eigenschaften, die von Windows gemeldet werden.

Systemeigenschaften

Diese Liste enthält die Systemdaten, die das Betriebssystem Ihres Knotens an ePolicy Orchestrator meldet. Überprüfen Sie die Details auf Ihrem System, bevor Sie von einer fehlerhaften Meldung ausgehen.

Agenten-GUID
CPU-Seriennummer
CPU-Geschwindigkeit (in MHz)
CPU-Typ
Benutzerdefinierte Eigenschaften 1-4
Kommunikationstyp
Standardsprache
Beschreibung
DNS-Name
Domänenname
Ausgeschlossene Tags
Freier Speicherplatz
Freier Arbeitsspeicher
Freier Speicherplatz auf dem Systemlaufwerk
Installierte Produkte
IP-Adresse
IPX-Adresse
Ist 64-Bit-OS
Letzter Reihenfolgefehler
Ist Laptop
Letzte Kommunikation
MAC-Adresse
Status "Verwaltet"
Verwaltungstyp
Anzahl der CPUs
Betriebssystem
OS-Build-Nummer
OS-OEM-Kennung
OS-Plattform
OS-Service Pack-Version
OS-Typ
OS-Version
Reihenfolgefehler
Server-Schlüssel
Subnetzadresse
Subnetzmaske
Systembeschreibung
Systemstandort
Systemname
Systemstruktursortierung
Tags
Zeitzone
Zu übertragen
Gesamter Speicherplatz
Gesamter physikalischer Arbeitsspeicher
Belegter Speicherplatz
Benutzername
Vdi

Agenten-Eigenschaften

Jedes McAfee-Produkt bestimmt die Eigenschaften, die es an ePolicy Orchestrator meldet. Darüber hinaus gibt es an, welche dieser Eigenschaften in eine Gruppe minimaler Eigenschaften aufgenommen werden. Diese Liste enthält die Arten von Produktdaten, die von der auf Ihrem System installierten McAfee-Software an ePolicy Orchestrator gemeldet werden. Falls Sie Fehler in den gemeldeten Werten finden, überprüfen Sie zunächst die Einzelheiten Ihrer Produkte, bevor Sie von einer fehlerhaften Meldung ausgehen.

Agenten-GUID

Schlüssel-Hash für die sichere Agent-zu-Server-Kommunikation

Agent-zu-Server-Kommunikationsintervall

Agenten-Reaktivierung

Kommunikationsport für Agenten-Reaktivierung

Cluster-Knoten

Zustand des Cluster-Dienstes

Cluster-Name

Cluster-Host

Cluster-Mitglieds-Knoten

Pfad der Cluster-Quorum-Ressource

Cluster-IP-Adresse

DAT-Version

Scan-Modul-Version

Automatischen Neustart erzwingen nach

HotFix/Patch-Version

Installationspfad

Sprache

Status der letzten Richtlinienerzwingung

Status der letzten Eigenschaftserfassung

Lizenzstatus

Aufforderung zum Neustart, wenn erforderlich

Richtlinienerzwingungsintervall

Produktversion

Plug-In-Version

"Jetzt ausführen" unterstützt

Service Pack

McAfee-Symbol in der Taskleiste anzeigen

SuperAgent als Relay-Dienst

SuperAgent-Funktion

SuperAgent-Repository

SuperAgent-Repository-Verzeichnis

Kommunikationsport für SuperAgent-Reaktivierung

Von McAfee Agent bereitgestellte Abfragen

McAfee Agent fügt einer ePolicy Orchestrator-Umgebung eine Reihe von Standardabfragen hinzu.

Die folgenden Abfragen werden in der freigegebenen Gruppe **McAfee Agent** installiert.

Tabelle 10-1 Von McAfee Agent bereitgestellte Abfragen

Abfrage	Beschreibung
Zusammenfassung Agenten-Kommunikation	Ein Kreisdiagramm mit verwalteten Systemen, das angibt, ob die Agenten innerhalb des letzten Tages mit dem McAfee ePO-Server kommuniziert haben.
Agentensteuerungsstatus	Ein Kreisdiagramm, das den Kommunikationsstatus der Agentensteuerung aus der letzten Stunde anzeigt.
Informationen zur Agenten-Statistik	Ein Balkendiagramm, das die folgenden Agenten-Statistiken anzeigt: • Anzahl der fehlgeschlagenen Verbindungen zu Relay-Servern • Anzahl der nach der maximal erlaubten Anzahl an Verbindungen vorgenommenen Verbindungsversuche zum Relay-Server • Die durch Verwendung der SuperAgent-Hierarchie eingesparte Netzwerkbandbreite
Zusammenfassung Agenten-Version	Ein Kreisdiagramm mit installierten Agenten – sortiert nach Versionsnummer – auf verwalteten Systemen.
Inaktive Agenten	Eine Tabelle, in der alle verwalteten Systeme aufgeführt sind, deren Agenten innerhalb des letzten Monats nicht kommuniziert haben.

Tabelle 10-1 Von McAfee Agent bereitgestellte Abfragen *(Fortsetzung)*

Abfrage	Beschreibung
Verwaltete Knoten mit Fehlern bei der Richtlinienerzwingung für Einzelprodukte	Ein Diagramm mit einem gruppierten Balken, das die maximale Anzahl verwalteter Knoten (im Abfragen-Generator angegeben) mit mindestens einem Fehler bei der Richtlinienerzwingung anzeigt. Sie können Fehler bei der Richtlinienerzwingung für Einzelprodukte im McAfee ePO 5.0-Server (oder höher) abfragen.
Verwaltete Knoten mit Fehlern bei der Eigenschaftserfassung für Einzelprodukte	Ein Diagramm mit einem gruppierten Balken, das die maximale Anzahl verwalteter Knoten (im Abfragen-Generator angegeben) mit mindestens einem Fehler bei der Erfassung von Eigenschaften anzeigt. Sie können Fehler bei der Erfassung von Eigenschaften für Einzelprodukte im McAfee ePO 5.0-Server (oder höher) abfragen.
Repositories und Auslastung in Prozent	Ein Kreisdiagramm, das die Auslastung einzelner Repositorys in Form eines Prozentwerts aus allen Repositorys anzeigt.
Repository-Verwendung basierend auf DAT- und Modulabruf	Ein gestapeltes Balkendiagramm, das den Abruf von DAT- und Moduldateien pro Repository anzeigt.
Systeme pro Agentensteuerung	Ein Kreisdiagramm, das die Anzahl verwalteter Systeme pro Agentensteuerung anzeigt.

Zulassen der Zwischenspeicherung von Anmeldeinformationen für die Agenten-Ausbringung

Um Agenten erfolgreich vom ePolicy Orchestrator-Server auf Systemen im Netzwerk ausbringen zu können, müssen Administratoren Anmeldeinformationen angeben. Sie können festlegen, ob die Anmeldeinformationen für die Agenten-Ausbringung für jeden Benutzer im Cache abgelegt werden sollen.

Wenn die Anmeldeinformationen eines Benutzers im Cache abgelegt werden, kann dieser Benutzer Agenten ausbringen, ohne seine Anmeldeinformationen erneut angeben zu müssen. Anmeldeinformationen werden benutzerspezifisch gespeichert, d. h. ein Benutzer kann Agenten nur dann ausbringen, wenn er seine eigenen Anmeldeinformationen zuvor schon einmal angegeben hat.

Vorgehensweise

Definitionen zu Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

1. Klicken Sie auf **Menü** | **Konfiguration** | **Server-Einstellungen**, wählen Sie in der Liste **Einstellungskategorien** den Eintrag **Anmeldeinformationen für Agenten-Ausbringung** aus, und klicken Sie dann auf **Bearbeiten**.
2. Aktivieren Sie das Kontrollkästchen, damit die Anmeldeinformationen für die Agenten-Ausbringung im Cache abgelegt werden.

Ändern der Ports für die Agenten-Kommunikation

Einige der für die Agenten-Kommunikation verwendeten Ports auf dem ePolicy Orchestrator-Server können Sie ändern.

Die Einstellungen für die folgenden Agenten-Kommunikationsports können Sie ändern:

- **Sicherer Port für Agent-zu-Server-Kommunikation**
- **Kommunikationsport für Agenten-Reaktivierung**
- **Kommunikationsport für Agenten-Übertragung**

Vorgehensweise

Definitionen zu Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

1. Klicken Sie auf **Menü** | **Konfiguration** | **Server-Einstellungen**, wählen Sie in der Liste **Einstellungskategorien** den Eintrag **Ports** aus, und klicken Sie dann auf **Bearbeiten**.
2. Legen Sie fest, ob der Port 443 als sicherer Port für die Agent-zu-Server-Kommunikation aktiviert werden soll, geben Sie die Ports ein, die für Agenten-Reaktivierungen und Agenten-Übertragungen verwendet werden sollen, und klicken Sie dann auf **Speichern**.

Anzeigen von Agenten- und Produkteigenschaften

Eine häufige Aufgabe bei der Fehlerbehebung besteht darin, zu überprüfen, dass die von Ihnen vorgenommenen Richtlinienänderungen mit den aus einem System abgerufenen Eigenschaften übereinstimmen.

Vorgehensweise

Definitionen zu Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

1. Klicken Sie auf **Menü** | **Systeme** | **Systemstruktur**.
2. Klicken Sie auf der Registerkarte **Systeme** auf die entsprechende Zeile des Systems, das Sie überprüfen möchten.

Es werden Informationen zu den Eigenschaften des Systems, den installierten Produkten und zum Agenten angezeigt. Die Multifunktionsleiste oben auf der Seite **Systeminformationen** enthält die Fenster **Zusammenfassung**, **Eigenschaften** und **Bedrohungsereignisse**. Es werden außerdem die Registerkarten **Systemeigenschaften**, **Produkte**, **Bedrohungsereignisse**, **McAfee Agent**, **Rogue System Detection** und **Verwandte Elemente** angezeigt.

Sicherheitsschlüssel

Mit Sicherheitsschlüsseln können Sie die Kommunikation und Inhalte in der von ePolicy Orchestrator verwalteten Umgebung überprüfen und authentifizieren.

Inhalt

Beschreibung und Funktionsweise von Sicherheitsschlüsseln

Der ePolicy Orchestrator-Server beruht auf drei Sicherheitsschlüsselpaaren.

Die drei Sicherheitsschlüsselpaare werden für folgende Zwecke verwendet:

- Authentifizieren der Agent-zu-Server-Kommunikation
- Überprüfen der Inhalte lokaler Repositories
- Überprüfen der Inhalte remoter Repositories

Mit dem geheimen Schlüssel jedes Paares werden Nachrichten oder Pakete an ihrer Quelle signiert, während sie mit dem öffentlichen Schlüssel des Paares an ihrem Ziel überprüft werden.

ASSC-Schlüssel (Schlüssel für sichere Agenten-Server-Kommunikation)

- Wenn der Agent zum ersten Mal mit dem Server kommuniziert, sendet er seinen öffentlichen Schlüssel an den Server.
- Von diesem Zeitpunkt an verwendet der Server den öffentlichen Schlüssel des Agenten, um Nachrichten zu überprüfen, die mit dem geheimen Schlüssel des Agenten signiert wurden.
- Eigene Nachrichten signiert der Server mit seinem eigenen geheimen Schlüssel, bevor er sie an den Agenten sendet.
- Der Agent überprüft dann die Nachrichten des Servers mithilfe des öffentlichen Schlüssels des Servers.
- Es kann mehrere Schlüsselpaare für die sichere Kommunikation geben, **aber nur ein Schlüsselpaar kann als Hauptschlüssel festgelegt werden**.
- Wenn der Aktualisierungs-Task für Client-Agenten-Schlüssel (**McAfee ePO Agent Key Updater**) ausgeführt wird, erhalten Agenten, die andere öffentliche Schlüssel verwenden, den aktuellen öffentlichen Schlüssel.
- Die vorhandenen Schlüssel werden auf Ihren McAfee ePO 5.0-Server migriert. Dabei spielt es keine Rolle, ob Sie ein Upgrade von Version 4.5 oder 4.6 aus durchführen.

Schlüsselpaare für lokales Master-Repository

- Mit dem geheimen Repository-Schlüssel wird das Paket signiert, bevor es in das Repository eingecheckt wird.
- Mit dem öffentlichen Repository-Schlüssel wird der Inhalt von Paketen im Master-Repository und verteilten Repository überprüft.
- Der Agent ruft bei jedem Client-Aktualisierungs-Task verfügbare neue Inhalte ab.
- Dieses Schlüsselpaar ist für jeden Server eindeutig.
- Durch Exportieren und Importieren von Schlüsseln zwischen Servern können Sie dasselbe Schlüsselpaar in einer Umgebung mit mehreren Servern verwenden.

Andere Repository-Schlüsselpaare

- Inhalte einer vertrauenswürdigen Quelle werden mit deren geheimen Schlüssel signiert, bevor die Inhalte an deren remotes Repository gesendet werden. Zu vertrauenswürdigen Quellen gehören die McAfee-Downloadseite und das SIA-Repository (Security Innovation Alliance) von McAfee.



Wenn dieser Schlüssel gelöscht wird, können Sie keine Abrufe mehr ausführen, selbst wenn Sie einen Schlüssel von einem anderen Server importieren. Bevor Sie diesen Schlüssel löschen oder überschreiben, müssen Sie sich deshalb vergewissern, dass Sie ihn an einem geschützten Ort gesichert haben.

- Mit dem öffentlichen Schlüssel des Agenten werden Inhalte überprüft, die aus dem remoten Repository empfangen werden.

Schlüsselpaar für Master-Repository

Der private Schlüssel für das Master-Repository signiert alle nicht signierten Inhalte im Master-Repository. Dieser Schlüssel ist eine Funktion von Agenten ab der Version 4.0.

Agenten ab der Version 4.0 verwenden den öffentlichen Schlüssel, um Repository-Inhalte zu überprüfen, die aus dem Master-Repository auf diesem McAfee ePO-Server stammen. Wenn der Inhalt nicht signiert oder mit einem unbekannten privaten Repository-Schlüssel signiert ist, wird der heruntergeladene Inhalt als unzulässig betrachtet und gelöscht.

Dieses Schlüsselpaar ist für jede Server-Installation eindeutig. Durch Exportieren und Importieren von Schlüsseln können Sie jedoch dasselbe Schlüsselpaar in einer Umgebung mit mehreren Servern verwenden. Mit dieser Maßnahme kann sichergestellt werden, dass Agenten immer eine Verbindung zu einem Ihrer Master-Repositories herstellen können, selbst wenn ein anderes Repository heruntergefahren ist.

Öffentliche Schlüssel für weitere Repositories

Bei anderen Schlüsseln als dem Hauptschlüsselpaar handelt es sich um die öffentlichen Schlüssel, mit denen Agenten Inhalte aus anderen Master-Repositories in Ihrer Umgebung oder McAfee-Quellsites überprüfen. Jeder Agent, der sich bei diesem Server meldet, verwendet die in der Liste **Öffentliche Schlüssel für weitere Repositories** aufgeführten Schlüssel zum Überprüfen von Inhalten, die von anderen McAfee ePO-Servern in Ihrem Unternehmen oder aus McAfee-eigenen Quellen stammen.

Wenn ein Agent Inhalte herunterlädt, die aus einer Quelle stammen, für die der Agent keinen entsprechenden öffentlichen Schlüssel besitzt, verwirft der Agent den Inhalt.

Diese Schlüssel sind eine neue Funktion. Nur Agenten ab der Version 4.0 können diese neuen Protokolle verwenden.

Verwalten von Repository-Schlüsseln

Gehen Sie wie in diesen Aufgaben beschrieben vor, um Repository-Schlüssel zu verwalten.

Aufgaben

- *Verwenden eines Master-Repository-Schlüsselpaares für alle Server* auf Seite 156
  Mithilfe der Option **Server-Einstellungen** können Sie in einer Umgebung mit mehreren Servern sicherstellen, dass alle McAfee ePO-Server und Agenten dasselbe Master-Repository-Schlüsselpaar verwenden.
- *Verwenden von Schlüsseln für das Master-Repository in Umgebungen mit mehreren Servern* auf Seite 157
  Mithilfe der **Server-Einstellungen** können Sie sicherstellen, dass Agenten auf Inhalte zugreifen können, die von beliebigen McAfee ePO-Servern in Ihrer Umgebung stammen.

Verwenden eines Master-Repository-Schlüsselpaares für alle Server

Mithilfe der Option **Server-Einstellungen** können Sie in einer Umgebung mit mehreren Servern sicherstellen, dass alle McAfee ePO-Server und Agenten dasselbe Master-Repository-Schlüsselpaar verwenden.

Dazu müssen Sie das Schlüsselpaar, das von allen Servern verwendet werden soll, zuerst exportieren und dann auf allen Servern in Ihrer Umgebung importieren.

Vorgehensweise

Definitionen zu Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

1. Klicken Sie auf **Menü** | **Konfiguration** | **Server-Einstellungen**, wählen Sie in der Liste **Einstellungskategorien** den Eintrag **Sicherheitsschlüssel** aus, und klicken Sie dann auf **Bearbeiten**.

   Die Seite **Sicherheitsschlüssel: Bearbeiten** wird angezeigt.

2. Klicken Sie neben **Schlüsselpaare für lokales Master-Repository** auf **Schlüsselpaar exportieren**.

3. Klicken Sie auf **OK**. Das Dialogfeld **Dateidownload** wird angezeigt.

4. Klicken Sie auf **Speichern**, wechseln Sie zum Speichern der ZIP-Datei mit den Schlüsseldateien für die sichere Kommunikation zu einem Speicherort, auf den von den anderen Servern aus zugegriffen werden kann, und klicken Sie dann auf **Speichern**.

5. Klicken Sie neben **Schlüssel importieren und sichern** auf **Importieren**.

6. Wechseln Sie zu der ZIP-Datei, in der sich die Dateien mit den exportierten Master-Repository-Schlüsseln befinden, und klicken Sie dann auf **Weiter**.

7. Vergewissern Sie sich, dass dies die Schlüssel sind, die Sie importieren möchten, und klicken Sie dann auf **Speichern**.

Das importierte Master-Repository-Schlüsselpaar ersetzt das vorhandene Schlüsselpaar auf diesem Server. Agenten verwenden das neue Schlüsselpaar nach dem nächsten Agenten-Aktualisierungs-Task. Nachdem das Master-Repository-Schlüsselpaar geändert wurde, muss eine sichere Agenten-Server-Kommunikation durchgeführt werden, bevor der Agent den neuen Schlüssel verwenden kann.

Verwenden von Schlüsseln für das Master-Repository in Umgebungen mit mehreren Servern

Mithilfe der **Server-Einstellungen** können Sie sicherstellen, dass Agenten auf Inhalte zugreifen können, die von beliebigen McAfee ePO-Servern in Ihrer Umgebung stammen.

Der Server signiert alle nicht signierten Inhalte, die in das Repository eingecheckt werden, mit dem privaten Schlüssel für das Master-Repository. Agenten überprüfen Inhalte, die aus Repositories in Ihrem Unternehmen oder McAfee-Quellsites abgerufen werden, mithilfe von öffentlichen Repository-Schlüsseln.

Das Schlüsselpaar für das Master-Repository ist für jede Installation von ePolicy Orchestrator eindeutig. Bei Einsatz mehrerer Server verwendet jeder Server einen anderen Schlüssel. Wenn die Agenten Inhalte herunterladen, die aus unterschiedlichen Master-Repositories stammen, müssen Sie sicherstellen, dass die Inhalte von den Agenten als zulässig erkannt werden.

Dazu haben Sie zwei Möglichkeiten:

- Verwenden Sie für alle Server und Agenten dasselbe Schlüsselpaar für das Master-Repository.
- Stellen Sie sicher, dass Agenten so konfiguriert sind, dass sie alle öffentlichen Repository-Schlüssel in Ihrer Umgebung erkennen.

Beim folgenden Vorgang wird das Schlüsselpaar aus einem McAfee ePO-Server auf einen anderen McAfee ePO-Ziel-Server exportiert und dann auf dem McAfee ePO-Ziel-Server importiert, wobei es das dort vorhandene Schlüsselpaar ersetzt.

Vorgehensweise

Definitionen zu Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

1. Klicken Sie auf dem McAfee ePO-Server, auf dem sich das Schlüsselpaar für das Master-Repository befindet, auf **Menü** | **Konfiguration** | **Server-Einstellungen**, wählen Sie in der Liste **Einstellungskategorien** den Eintrag **Sicherheitsschlüssel** aus, und klicken Sie dann auf **Bearbeiten**.

   Die Seite **Sicherheitsschlüssel: Bearbeiten** wird angezeigt.
2. Klicken Sie neben **Schlüsselpaare für lokales Master-Repository** auf **Schlüsselpaar exportieren**.
3. Klicken Sie auf **OK**. Das Dialogfeld **Dateidownload** wird angezeigt.
4. Klicken Sie auf **Speichern**, und wechseln Sie dann zu einem Speicherort auf dem McAfee ePO-Ziel-Server, an dem die ZIP-Datei gespeichert werden soll.
5. Ändern Sie gegebenenfalls den Namen der Datei, und klicken Sie dann auf **Speichern**.
6. Klicken Sie auf dem McAfee ePO-Ziel-Server, auf dem Sie das Schlüsselpaar für das Master-Repository laden möchten, auf **Menü** | **Konfiguration** | **Server-Einstellungen**, wählen Sie in der Liste **Einstellungskategorien** den Eintrag **Sicherheitsschlüssel** aus, und klicken Sie dann auf **Bearbeiten**.

   Die Seite **Sicherheitsschlüssel: Bearbeiten** wird angezeigt.
7. Klicken Sie neben **Schlüssel importieren und sichern** auf **Importieren**.
8. Wechseln Sie neben **Datei auswählen** zu dem von Ihnen gespeicherten Schlüsselpaar für das Master-Repository, wählen Sie es aus, und klicken Sie dann auf **Weiter**.
9. Überprüfen Sie, ob die Angaben korrekt sind, und klicken Sie dann auf **Speichern**. Das neue Hauptschlüsselpaar wird in der Liste neben **Schlüssel für sichere Agenten-Server-Kommunikation** angezeigt.
10. Wählen Sie in der Liste die Datei aus, die Sie in den vorherigen Schritten importiert haben, und klicken Sie auf **Als Master festlegen**. Dadurch wird das neu importierte Schlüsselpaar als Hauptschlüsselpaar festgelegt.
11. Klicken Sie auf **Speichern**, um den Vorgang abzuschließen.

ASSC-Schlüssel (Schlüssel für sichere Agenten-Server-Kommunikation)

Mithilfe von ASSC-Schlüsseln (Agent-Server Secure Communication, sichere Agenten-Server-Kommunikation) können Agenten sicher mit dem Server kommunizieren.

Sie können jedes beliebige ASSC-Schlüsselpaar als Hauptschlüssel festlegen. Das ist das Schlüsselpaar, das derzeit allen ausgebrachten Agenten zugewiesen ist. Vorhandene Agenten, die andere Schlüssel in der Liste **Schlüssel für sichere Agenten-Server-Kommunikation** verwenden, wechseln nur dann zum neuen Hauptschlüssel, wenn ein Aktualisierungs-Task für Client-Agenten-Schlüssel geplant ist und ausgeführt wird.



Löschen Sie ältere Schlüssel erst dann, wenn alle Agenten den neuen Hauptschlüssel übernommen haben.



Ältere Windows-Agenten als Version 4.0 werden nicht unterstützt.

Arbeiten mit ASSC-Schlüsseln

Gehen Sie bei der Verwaltung und Verwendung von ASSC-Schlüsseln in Ihrer Umgebung wie in den folgenden Aufgaben beschrieben vor.

Aufgaben

- *Verwalten von ASSC-Schlüsseln* auf Seite 159
  Sie können Schlüssel für die sichere Agenten-Server-Kommunikation (Agent-Server Secure Communication, ASSC) in den **Server-Einstellungen** generieren, exportieren, importieren und löschen.
- *Anzeigen von Systemen, die ein ASSC-Schlüsselpaar verwenden* auf Seite 161
  Sie können die Systeme anzeigen, deren Agenten ein bestimmtes ASSC-Schlüsselpaar aus der Liste **Schlüssel für sichere Agenten-Server-Kommunikation** verwenden.
- *Verwenden desselben ASSC-Schlüsselpaares für alle Server und Agenten* auf Seite 162
  Sie sollten sicherstellen, dass alle McAfee ePO-Server und Agenten dasselbe ASSC-Schlüsselpaar verwenden.
- *Verwenden verschiedener ASSC-Schlüsselpaare für jeden McAfee ePO-Server* auf Seite 162
  Sie können für jeden McAfee ePO-Server ein anderes ASSC-Schlüsselpaar verwenden, um sicherzustellen, dass alle Agenten mit den erforderlichen McAfee ePO-Servern in einer Umgebung kommunizieren können, in der jeder Server über ein eigenes, eindeutiges ASSC-Schlüsselpaar verfügen muss.

Verwalten von ASSC-Schlüsseln

Sie können Schlüssel für die sichere Agenten-Server-Kommunikation (Agent-Server Secure Communication, ASSC) in den **Server-Einstellungen** generieren, exportieren, importieren und löschen.

Vorgehensweise

Definitionen zu Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

1. Klicken Sie auf **Menü** | **Konfiguration** | **Server-Einstellungen**, und wählen Sie in der Liste **Einstellungskategorien** den Eintrag **Sicherheitsschlüssel** aus.

   Die Seite **Sicherheitsschlüssel: Bearbeiten** wird angezeigt.

2. Wählen Sie eine der folgenden Aktionen aus.

Aktion	Vorgehensweise
Generieren und Verwenden neuer ASSC-Schlüsselpaare	Gehen Sie wie nachfolgend beschrieben vor, um neue ASSC-Schlüsselpaare zu generieren. 1 Klicken Sie neben der Liste **Schlüssel für sichere Agenten-Server-Kommunikation** auf **Neuer Schlüssel**. Geben Sie in dem Dialogfeld den Namen des Sicherheitsschlüssels ein. 2 Wenn der neue Schlüssel von vorhandenen Agenten verwendet werden soll, wählen Sie den Schlüssel in der Liste aus, und klicken Sie dann auf **Als Master festlegen**. Agenten verwenden den neuen Schlüssel nach Abschluss des nächsten Agenten-Aktualisierungs-Tasks. Wenn der Server Agenten der Version 4.6 verwaltet, müssen Sie sicherstellen, dass Version 4.6 des Agenten-Schlüsselaktualisierungspakets (Agent Key Updater) in das Master-Repository eingecheckt ist. Bei umfangreicheren Installationen sollten neue Hauptschlüsselpaare nur dann generiert und verwendet werden, wenn es dafür gute Gründe gibt. Sie sollten dieses Verfahren phasenweise durchführen, damit Sie den Fortschritt genauer überwachen können. 3 Löschen Sie den alten Schlüssel, nachdem er von keinem der Agenten mehr verwendet wird. In der Liste mit den Schlüsseln wird rechts von jedem Schlüssel angezeigt, von wie vielen Agenten er gerade verwendet wird. 4 Sichern Sie alle Schlüssel.
Exportieren von ASSC-Schlüsseln	Gehen Sie wie nachfolgend beschrieben vor, um ASSC-Schlüssel aus einem McAfee ePO-Server auf einen anderen McAfee ePO-Server zu exportieren, sodass Agenten auf diesen neuen McAfee ePO-Server zugreifen können. 1 Wählen Sie in der Liste **Schlüssel für sichere Agenten-Server-Kommunikation** einen Schlüssel aus, und klicken Sie dann auf **Exportieren**. Das Dialogfeld **Schlüssel für sichere Agenten-Server-Kommunikation exportieren** wird angezeigt. 2 Klicken Sie auf **OK**. Sie werden von Ihrem Browser gefragt, ob die Datei SR<SERVER-NAME>.ZIP in den angegebenen Speicherort heruntergeladen werden soll. Je nach dem verwendeten Internet-Browser (oder wenn Sie einen Standardspeicherort für alle Download-Vorgänge angegeben haben) kann diese Datei auch automatisch in diesem Speicherort gespeichert werden.

Aktion	Vorgehensweise
Importieren von ASSC-Schlüsseln	Gehen Sie wie nachfolgend beschrieben vor, um ASSC-Schlüssel zu importieren, die auf einem anderen McAfee ePO-Server exportiert wurden. Damit können Agenten von jenem Server auf diesen McAfee ePO-Server zugreifen. 1 Klicken Sie auf **Importieren**. Die Seite **Schlüssel importieren** wird angezeigt. 2 Wechseln Sie in den Speicherort, in dem Sie den Schlüssel gespeichert haben (in der Standardeinstellung auf dem Desktop), wählen Sie den Schlüssel aus, und klicken Sie dann auf **Öffnen**. 3 Klicken Sie auf **Weiter**, und überprüfen Sie die auf der Seite **Zusammenfassung** angezeigten Informationen. 4 Klicken Sie auf **Speichern**.
Festlegen eines ASSC-Schlüsselpaares als Master	Gehen Sie wie nachfolgend beschrieben vor, um ein anderes Schlüsselpaar aus der Liste **Schlüssel für sichere Agenten-Server-Kommunikation** als Master festzulegen. Führen Sie diesen Schritt nach dem Importieren oder Generieren eines neuen Schlüsselpaares durch. 1 Wählen Sie in der Liste **Schlüssel für sichere Agenten-Server-Kommunikation** einen Schlüssel aus, und klicken Sie dann auf **Als Master festlegen**. 2 Erstellen Sie für die Agenten einen Aktualisierungs-Task, der sofort ausgeführt wird, sodass die Agenten nach der nächsten Agent-zu-Server-Kommunikation aktualisiert werden. Stellen Sie sicher, dass das Aktualisierungspaket für den Agenten-Schlüssel in das Master-Repository eingecheckt ist und in alle von ePolicy Orchestrator verwalteten verteilten Repositories repliziert wurde. Agenten beginnen das neue Schlüsselpaar zu verwenden, sobald der nächste Aktualisierungs-Task für den jeweiligen Agenten abgeschlossen ist. Sie können in der Liste jederzeit sehen, welche Agenten Schlüsselpaare zur sicheren Kommunikation zwischen Agent und Server verwenden. 3 Sichern Sie alle Schlüssel.
Löschen von ASSC-Schlüsseln	Löschen Sie keine Schlüssel, die noch von Agenten verwendet werden. Andernfalls können diese Agenten nicht mit dem Server kommunizieren. 1 Wählen Sie in der Liste **Schlüssel für sichere Agenten-Server-Kommunikation** den Schlüssel aus, den Sie entfernen möchten, und klicken Sie dann auf **Löschen**. Das Dialogfeld **Schlüssel löschen** wird angezeigt. 2 Klicken Sie auf **OK**, um das Schlüsselpaar auf diesem Server zu löschen.

Anzeigen von Systemen, die ein ASSC-Schlüsselpaar verwenden

Sie können die Systeme anzeigen, deren Agenten ein bestimmtes ASSC-Schlüsselpaar aus der Liste **Schlüssel für sichere Agenten-Server-Kommunikation** verwenden.

Nachdem Sie ein bestimmtes Schlüsselpaar als Master festgelegt haben, möchten Sie eventuell die Systeme anzeigen, die noch das vorherige Schlüsselpaar verwenden. Löschen Sie ein Schlüsselpaar erst dann, wenn Sie wissen, dass es von keinem Agenten mehr verwendet wird.

Definitionen zu Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

Vorgehensweise

1. Klicken Sie auf **Menü** | **Konfiguration** | **Server-Einstellungen**, wählen Sie in der Liste **Einstellungskategorien** den Eintrag **Sicherheitsschlüssel** aus, und klicken Sie dann auf **Bearbeiten**.

   Die Seite **Sicherheitsschlüssel: Bearbeiten** wird angezeigt.

2. Wählen Sie in der Liste **Schlüssel für sichere Agenten-Server-Kommunikation** einen Schlüssel aus, und klicken Sie dann auf **Agenten anzeigen**. Die Seite **Systeme, die diesen Schlüssel verwenden** wird angezeigt.

Auf dieser Seite sind alle Systeme aufgeführt, deren Agenten den ausgewählten Schlüssel verwenden.

Verwenden desselben ASSC-Schlüsselpaares für alle Server und Agenten

Sie sollten sicherstellen, dass alle McAfee ePO-Server und Agenten dasselbe ASSC-Schlüsselpaar verwenden.



Wenn in Ihrer Umgebung eine größere Anzahl von verwalteten Systemen vorhanden ist, sollte dieser Vorgang phasenweise durchgeführt werden, damit Sie Agenten-Aktualisierungen überwachen können.

Gehen Sie wie folgt vor, um sicherzustellen, dass alle McAfee ePO-Server und Agenten dasselbe ASSC-Schlüsselpaar verwenden.

1. Erstellen Sie einen Agenten-Aktualisierungs-Task.
2. Exportieren Sie die ausgewählten Schlüssel auf dem ausgewählten McAfee ePO-Server.
3. Importieren Sie die exportierten Schlüssel auf allen anderen Servern.
4. Legen Sie den importierten Schlüssel auf allen Servern als Master fest.
5. Führen Sie zwei Agenten-Reaktivierungen durch.
6. Wenn alle Agenten mit den neuen Schlüsseln arbeiten, können Sie die nicht mehr verwendeten Schlüssel löschen.
7. Sichern Sie alle Schlüssel.

Verwenden verschiedener ASSC-Schlüsselpaare für jeden McAfee ePO-Server

Sie können für jeden McAfee ePO-Server ein anderes ASSC-Schlüsselpaar verwenden, um sicherzustellen, dass alle Agenten mit den erforderlichen McAfee ePO-Servern in einer Umgebung kommunizieren können, in der jeder Server über ein eigenes, eindeutiges ASSC-Schlüsselpaar verfügen muss.



Agenten können nicht mit mehreren Servern gleichzeitig kommunizieren. Der McAfee ePO-Server kann mehrere Schlüssel besitzen, um mit verschiedenen Agenten zu kommunizieren, aber nicht umgekehrt. Agenten können nicht über mehrere Schlüssel verfügen, um mit mehreren McAfee ePO-Servern zu kommunizieren.

Definitionen zu Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

Vorgehensweise

1. Exportieren Sie von jedem McAfee ePO-Server in Ihrer Umgebung das ASSC-Hauptschlüsselpaar in einen temporären Speicherort.
2. Importieren Sie jedes dieser Schlüsselpaare auf die einzelnen McAfee ePO-Server.

Sichern und Wiederherstellen von Schlüsseln

Sie sollten in regelmäßigen Abständen sämtliche Sicherheitsschlüssel sichern und stets eine Sicherung erstellen, bevor Sie Änderungen an den wichtigsten Verwaltungseinstellungen vornehmen.

Bewahren Sie die Sicherung in einem sicheren Speicherort im Netzwerk auf, sodass die Schlüssel leicht wiederhergestellt werden können, falls sie auf dem McAfee ePO-Server verloren gehen.

Vorgehensweise

Definitionen zu Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

1. Klicken Sie auf **Menü** | **Konfiguration** | **Server-Einstellungen**, wählen Sie in der Liste **Einstellungskategorien** den Eintrag **Sicherheitsschlüssel** aus, und klicken Sie dann auf **Bearbeiten**.

   Die Seite **Sicherheitsschlüssel: Bearbeiten** wird angezeigt.

2. Wählen Sie eine der folgenden Aktionen aus.

Aktionen	Vorgehensweise
Sichern aller Sicherheitsschlüssel	1 Klicken Sie im unteren Teil der Seite auf **Alle sichern**. Das Dialogfeld **Schlüsselspeicher sichern** wird angezeigt. 2 Sie können optional ein Kennwort zum Verschlüsseln der Schlüsselspeicher-ZIP-Datei eingeben oder auf **OK** klicken, um die Dateien in unverschlüsselter Textform zu speichern. 3 Klicken Sie im Dialogfeld **Dateidownload** auf **Speichern**, um eine ZIP-Datei mit allen Sicherheitsschlüsseln zu erstellen. Das Dialogfeld **Speichern unter** wird angezeigt. 4 Wechseln Sie zu einem sicheren Netzwerkspeicherort, in dem die ZIP-Datei gespeichert werden soll, und klicken Sie dann auf **Speichern**.
Wiederherstellen von Sicherheitsschlüsseln	1 Klicken Sie unten auf der Seite auf **Alle wiederherstellen**. Die Seite **Sicherheitsschlüssel wiederherstellen** wird angezeigt. 2 Wechseln Sie zu der ZIP-Datei, in der sich die Sicherheitsschlüssel befinden, wählen Sie die Datei aus, und klicken Sie dann auf **Weiter**. Die Seite **Zusammenfassung** des Assistenten **Sicherheitsschlüssel wiederherstellen** wird angezeigt. 3 Wechseln Sie zu den Schlüsseln, mit denen Sie Ihre vorhandenen Schlüssel ersetzen möchten, und klicken Sie auf **Weiter**. 4 Klicken Sie auf **Wiederherstellen**. Die Seite **Sicherheitsschlüssel: Bearbeiten** wird erneut angezeigt. 5 Wechseln Sie zu einem sicheren Netzwerkspeicherort, in dem die ZIP-Datei gespeichert werden soll, und klicken Sie dann auf **Speichern**.
Wiederherstellen von Sicherheitsschlüsseln aus einer Sicherungsdatei	1 Klicken Sie unten auf der Seite auf **Alle wiederherstellen**. Die Seite **Sicherheitsschlüssel wiederherstellen** wird angezeigt. 2 Wechseln Sie zu der ZIP-Datei, in der sich die Sicherheitsschlüssel befinden, wählen Sie die Datei aus, und klicken Sie dann auf **Weiter**. Die Seite **Zusammenfassung** des Assistenten **Sicherheitsschlüssel wiederherstellen** wird angezeigt. 3 Wechseln Sie zu der ZIP-Sicherungsdatei, wählen Sie sie aus, und klicken Sie anschließend auf **Weiter**. 4 Klicken Sie unten auf der Seite auf **Alle wiederherstellen**. Der Assistent **Sicherheitsschlüssel wiederherstellen** wird geöffnet. 5 Wechseln Sie zu der ZIP-Sicherungsdatei, wählen Sie sie aus, und klicken Sie anschließend auf **Weiter**. 6 Überprüfen Sie, ob die Schlüssel in dieser Datei mit denjenigen identisch sind, mit denen Sie die vorhandenen Schlüssel überschreiben möchten, und klicken Sie anschließend auf **Wiederherstellen**.

11 Software-Manager

Mit dem Software-Manager können Sie McAfee-Software sowie Software-Komponenten überprüfen und erwerben.

Inhalt

Inhalt des Software-Managers

Mit dem Software-Manager müssen Sie nicht mehr auf die McAfee-Website für den Produkt-Download zugreifen, um neue McAfee-Software und Software-Aktualisierungen zu erhalten.

Sie können mit dem Software-Manager Folgendes herunterladen:

- Lizenzierte Software
- Test-Software
- Software-Aktualisierungen
- Produktdokumentationen



DAT-Dateien und Scan-Module sind nicht über den Software-Manager erhältlich.

Lizenzierte Software

Lizenzierte Software ist jegliche Software, die Ihr Unternehmen von McAfee erworben hat. Im **Software-Manager** in der ePolicy Orchestrator-Konsole wird in der Produktkategorie **Nicht eingecheckte Software** jegliche Software angezeigt, für die Ihr Unternehmen eine Lizenz besitzt, die jedoch noch nicht auf dem Server installiert ist. Die neben jeder Unterkategorie in der Liste **Produktkategorien** angezeigte Zahl zeigt an, wie viele Produkte verfügbar sind.

Test-Software

Test-Software ist Software, für die Ihr Unternehmen gegenwärtig keine Lizenz besitzt. Sie können auf dem Server Test-Software installieren. Deren Funktionalität kann jedoch eingeschränkt sein, bis Sie eine Produktlizenz erwerben.

Software-Aktualisierungen

Wenn für die von Ihnen verwendete Software eine neue Aktualisierung veröffentlicht wird, können Sie den **Software-Manager** verwenden, um neue Pakete und Erweiterungen einzuchecken. Verfügbare Software-Aktualisierungen sind in der Kategorie **Aktualisierungen verfügbar** aufgeführt.

Produktdokumentationen

Neue und aktualisierte Produktdokumentationen können über den **Software-Manager** bezogen werden. Hilfeerweiterungen können automatisch installiert werden. Außerdem können über den **Software-Manager** auch PDF- und HTML-Dokumentationen (wie Produkthandbücher und Versionsinformationen) heruntergeladen werden.

Informationen zu Abhängigkeiten bei Software-Komponenten

Viele der Software-Produkte, die Sie zur Nutzung mit Ihrem McAfee ePO-Server installieren können, verfügen über vordefinierte Abhängigkeiten zu anderen Komponenten. Abhängige Elemente für Produkterweiterungen werden automatisch installiert. Für alle anderen Produktkomponenten müssen Sie die Liste der Abhängigkeiten auf der Seite **Komponentendetails** überprüfen und diese Komponenten dann vorher installieren.

Einchecken, Aktualisieren und Entfernen von Software mit dem Software-Manager

Im Software-Manager können Sie von McAfee verwaltete Produktkomponenten auf Ihrem Server einchecken, aktualisieren und entfernen.

Im Software-Manager kann sowohl auf lizenzierte Software als auch auf Testversionen zugegriffen werden.



Welche Software verfügbar ist und ob sie sich in der Kategorie **Lizenziert** oder **Test** befindet, hängt von Ihrem Lizenzschlüssel ab. Weitere Informationen erhalten Sie von Ihrem Administrator.

Vorgehensweise

Definitionen zu Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

1. Klicken Sie auf **Menü** | **Software** | **Software-Manager**.
2. Wählen Sie auf der Seite **Software-Manager** in der Liste **Produktkategorien** eine der folgenden Kategorien aus, oder suchen Sie Ihre Software mithilfe des Suchfelds:
   - **Aktualisierungen verfügbar** – In dieser Kategorie sind alle verfügbaren Aktualisierungen für lizenzierte Software-Komponenten aufgeführt, die auf diesem ePolicy Orchestrator-Server bereits installiert oder eingecheckt sind.
   - **Eingecheckte Software** – In dieser Kategorie wird sämtliche Software angezeigt (sowohl vom Typ **Lizenziert** als auch **Test**), die auf diesem Server installiert oder eingecheckt ist.

     Wenn eine kürzlich für ein Produkt hinzugefügte Lizenz als **Test** aufgeführt ist, klicken Sie **Aktualisieren**, damit der Wert bei **Lizenziert** aktualisiert und das Produkt unter **Eingecheckte Software** als **Lizenziert** geführt wird.
   - **Nicht eingecheckte Software** – In dieser Kategorie wird Software aufgeführt, die verfügbar, auf diesem Server jedoch nicht installiert ist.
   - **Software (nach Beschriftung)** – In dieser Kategorie ist Software nach ihrer Funktion laut Beschreibung von McAfee-Produkt-Suites aufgeführt.
3. Wenn Sie die richtige Software gefunden haben, klicken Sie auf eine der folgenden Optionen:
   - **Herunterladen**, um die Produktdokumentation in einen Speicherort in Ihrem Netzwerk herunterzuladen.
   - **Einchecken**, um eine Produkterweiterung oder ein Paket auf diesem Server einzuchecken.

- **Aktualisieren**, um ein Paket oder eine Erweiterung zu aktualisieren, das bzw. die derzeit auf diesem Server installiert oder eingecheckt ist.
- **Entfernen**, um ein Paket oder eine Erweiterung zu deinstallieren, das bzw. die derzeit auf diesem Server installiert oder eingecheckt ist.

4 Lesen Sie auf der Seite **Zusammenfassung zum Einchecken der Software** die Produktdetails und den Endbenutzer-Lizenzvertrag (EULA) durch, akzeptieren Sie ihn, und klicken Sie dann auf **OK**, um den Vorgang abzuschließen.

Überprüfen der Produktkompatibilität

Sie können eine Produktkompatibilitätsüberprüfung so konfigurieren, dass automatisch eine Produktkompatibilitätsliste von McAfee heruntergeladen wird. In dieser Liste sind Produkte aufgeführt, die in Ihrer ePolicy Orchestrator-Umgebung nicht mehr kompatibel sind.

ePolicy Orchestrator führt diese Überprüfung jedes Mal durch, wenn die Installation und der Start einer Erweiterung zu einem unerwünschten Zustand Ihres Servers führen könnten. Diese Überprüfung findet in den folgenden Szenarien statt:

- Während eines Upgrades von einer früheren Version von ePolicy Orchestrator auf die Version 5.0 (oder höher).
- Wenn eine Erweiterung über das Menü **Erweiterungen** installiert wird.
- Bevor eine neue Erweiterung vom Software-Manager abgerufen wird.
- Wenn eine neue Kompatibilitätsliste von McAfee empfangen wird.
- Wenn das Tool zur Datenmigration ausgeführt wird. Ausführliche Informationen dazu finden Sie im *Installationshandbuch von McAfee ePolicy Orchestrator 5.0.0*.

Produktkompatibilitätsüberprüfung

Bei der Produktkompatibilitätsüberprüfung wird anhand einer als Produktkompatibilitätsliste bezeichneten XML-Datei festgestellt, welche Produkterweiterungen zu einer Version von ePolicy Orchestrator *nicht kompatibel* sind.

Eine erste Liste ist bereits in dem ePolicy Orchestrator-Paket enthalten, das Sie von der McAfee-Website heruntergeladen haben. Beim Setup von ePolicy Orchestrator während einer Installation oder eines Upgrades lädt ePolicy Orchestrator automatisch eine aktuelle Liste der kompatiblen Erweiterungen von einer vertrauenswürdigen McAfee-Quelle über das Internet herunter. Wenn die Internetquelle nicht verfügbar ist oder die Liste nicht verifiziert werden kann, verwendet ePolicy Orchestrator die letzte gespeicherte Version.



Der ePolicy Orchestrator-Server aktualisiert die Produktkompatibilitätsliste (eine kleine Datei) einmal täglich im Hintergrund.

Fehlerbehebung

Wenn Sie die Liste der nicht kompatiblen Erweiterungen über das Installationsprogramm oder das Upgrade-Kompatibilitätsprogramm von ePolicy Orchestrator anzeigen, werden Sie benachrichtigt, wenn eine bekannte Ersatzerweiterung verfügbar ist.

In einigen Fällen kann während eines Upgrades folgende Situation auftreten:

- Eine Erweiterung blockiert das Upgrade und muss entfernt oder ersetzt werden, bevor das Upgrade fortgesetzt werden kann.
- Eine Erweiterung ist deaktiviert und muss nach Abschluss des ePolicy Orchestrator-Upgrades aktualisiert werden.

Ausführlichere Informationen dazu finden Sie unter *Blockierte oder deaktivierte Erweiterungen*.

Deaktivieren der automatischen Aktualisierungen

Sie können die automatischen Aktualisierungen der Produktkompatibilitätsliste deaktivieren, um zu verhindern, dass eine neue Liste heruntergeladen wird.

Der Download erfolgt im Rahmen von Hintergrundaufgaben oder beim Aktualisieren von Inhalten des Software-Managers. Diese Deaktivierung ist besonders nützlich, wenn Ihr McAfee ePO-Server über keinen Internetzugriff für Datenempfang verfügt. Ausführliche Informationen dazu finden Sie unter *Ändern der Einstellungen für den Download der Produktkompatibilitätsliste*.



Wenn die Einstellung für den Download der Produktkompatibilitätsliste erneut aktiviert wird, werden auch die automatischen Aktualisierungen der Produktkompatibilitätsliste im Software-Manager wieder aktiviert.

Verwenden einer manuell heruntergeladenen Produktkompatibilitätsliste

Eine manuell heruntergeladene Produktkompatibilitätsliste können Sie zum Beispiel dann verwenden, wenn Ihr ePolicy Orchestrator-Server über keinen Internetzugriff verfügt.

Die Liste können Sie bei den folgenden Gelegenheiten manuell herunterladen:

- Wenn Sie ePolicy Orchestrator installieren. Ausführliche Informationen dazu finden Sie unter *Blockierte oder deaktivierte Erweiterungen*.
- Wenn Sie über **Server-Einstellungen | Produktkompatibilitätsliste** eine Produktkompatibilitätsliste manuell hochladen. Diese Liste ist dann sofort nach dem Hochladen gültig.

  Deaktivieren Sie die automatische Aktualisierung der Liste, um zu verhindern, dass die manuell heruntergeladene Produktkompatibilitätsliste überschrieben wird. Ausführliche Informationen dazu finden Sie unter *Ändern der Einstellungen für den Download der Produktkompatibilitätsliste*.

- Klicken Sie auf PRODUCTCOMPATIBILITYLIST.XML, um die Liste manuell herunterzuladen.

Blockierte oder deaktivierte Erweiterungen

Wenn eine Erweiterung in der Produktkompatibilitätsliste blockiert ist, verhindert sie das Software-Upgrade von ePolicy Orchestrator. Wenn eine Erweiterung deaktiviert ist, wird das Upgrade dadurch nicht blockiert. Die Erweiterung wird nach Abschluss des Upgrades jedoch erst aktiviert, wenn eine bekannte Ersatzerweiterung installiert wurde.

Befehlszeilenoptionen für die Installation der Produktkompatibilitätsliste

Mithilfe der folgenden Befehlszeilenoptionen für den Befehl `SETUP.EXE` können Sie Downloads der Produktkompatibilitätsliste konfigurieren.

Option	Definition
`setup.exe DISABLEPRODCOMPATUPDATE=1`	Deaktiviert das automatische Herunterladen der Produktkompatibilitätsliste von der McAfee-Website.
`setup.exe PRODCOMPATXML=<vollständiger_Dateiname_inklusive_Pfad>`	Gibt eine alternative Produktkompatibilitätslisten-Datei an.



Beide Befehlszeilenoptionen können gemeinsam in einer Befehlszeichenfolge verwendet werden.

Ändern der Einstellungen für den Download der Produktkompatibilitätsliste

Sie können die Produktkompatibilitätsliste entweder aus dem Internet herunterladen oder eine manuell heruntergeladene Liste verwenden, um Produkte zu ermitteln, die in Ihrer ePolicy Orchestrator-Umgebung nicht mehr kompatibel sind.

Bevor Sie beginnen

Als manuell heruntergeladene Produktkompatibilitätslisten sind nur gültige XML-Dateien von McAfee zulässig.



Falls Sie in der XML-Datei der Produktkompatibilitätsliste Änderungen vornehmen, wird die Datei ungültig.

Vorgehensweise

Definitionen zu Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

1. Klicken Sie auf **Menü** | **Konfiguration** | **Server-Einstellungen**, wählen Sie in der Liste **Einstellungskategorien** den Eintrag **Produktkompatibilitätsliste** aus, und klicken Sie dann auf **Bearbeiten**.

   Eine Seite wird angezeigt, auf der die deaktivierten nicht kompatiblen Erweiterungen in einer Tabelle aufgelistet sind.

2. Klicken Sie auf **Deaktiviert**, um den automatischen und regelmäßigen Download der Produktkompatibilitätsliste von McAfee zu stoppen.

3. Klicken Sie auf **Durchsuchen**, wechseln Sie zu **Produktkompatibilitätsliste hochladen**, und klicken Sie dann auf **Speichern**.

Nachdem Sie den automatischen Download der Produktkompatibilitätsliste deaktiviert haben, verwendet Ihr McAfee ePO-Server so lange die gleiche Liste, bis Sie eine neue Liste hochladen oder den Server mit dem Internet verbinden und das automatische Herunterladen wieder aktivieren.

12 Produktausbringung

ePolicy Orchestrator vereinfacht die Ausbringung von Sicherheitsprodukten auf den verwalteten Systemen in einem Netzwerk, indem es eine Benutzeroberfläche bereitstellt, in der Ausbringungen konfiguriert und geplant werden können.

Zum Ausbringen von Produkten mittels ePolicy Orchestrator können Sie nach zwei Methoden vorgehen:

- Mithilfe von Produktausbringungsprojekten (neu in McAfee ePO 5.0), die den Ausbringungsvorgang vereinfachen und zusätzliche Funktionen zur Verfügung stellen.
- Mithilfe individuell erstellter und verwalteter Client-Task-Objekte und Tasks. Weitere Informationen zu dieser Methode finden Sie unter *Ausbringungs-Tasks* in *Client- und Server-Tasks*.

Inhalt

Auswählen einer Methode zur Produktausbringung

Welche Methode zur Produktausbringung für Sie am besten geeignet ist, hängt von der bereits vorhandenen Konfiguration ab.

Produktausbringungsprojekte zeichnen sich durch einen vereinfachten Ablauf sowie umfangreichere Funktionen zur Ausbringungen auf Systemen aus, die von ePolicy Orchestrator verwaltet werden. Allerdings können Produktausbringungsprojekte nicht in Kombination mit oder zum Verwalten von Client-Task-Objekten und Tasks verwendet werden, die mit einer älteren Software als Version 5.0 erstellt wurden.

Wenn Sie Client-Tasks und Objekte, die außerhalb eines Produktausbringungsprojekts erstellt wurden, beibehalten und weiter nutzen möchten, müssen Sie die Client-Task-Objektbibliothek und die -zuweisungsschnittstellen verwenden. Sie können Ihre vorhandenen Tasks und Objekte weiter behalten, während Sie neue Ausbringungen mithilfe der Schnittstelle für Produktausbringungsprojekte erstellen.

Weitere Informationen über das Ausbringen von Produkten mithilfe von Client-Task-Objekten finden Sie unter *Ausbringungs-Tasks* im Kapitel *Client- und Server-Tasks*.

Vorteile von Produktausbringungsprojekten

Produktausbringungsprojekte vereinfachen die Ausbringung von Sicherheitsprodukten auf verwalteten Systemen, da sie den für die Planung und Wartung von Ausbringungen im Netzwerk erforderlichen Zeit- und Verwaltungsaufwand verringern.

Indem bei Produktausbringungsprojekten viele der Schritte zusammengefasst werden, die zum Erstellen und Verwalten der einzelnen Produktausbringungs-Tasks erforderlich sind, wird der Ausbringungsvorgang erheblich vereinfacht. Darüber hinaus ermöglichen diese Projekte folgende Aufgaben:

- **Ausführen einer Ausbringung auf beliebig vielen Systemen.** Sie können Ausbringungsprojekte so konfigurieren, dass Produkte auf neu hinzugefügten Systemen automatisch ausgebracht werden, wenn diese neuen Systeme mit den von Ihnen festgelegten Kriterien übereinstimmen.
- **Anhalten einer laufenden Ausbringung.** Sie haben nun die Möglichkeit, eine bereits begonnene Ausbringung bei Bedarf anzuhalten. Anschließend können Sie die Ausbringung zu jedem gewünschten Zeitpunkt wieder fortsetzen.
- **Deinstallieren eines bereits ausgebrachten Produkts.** Wenn Sie nach Abschluss eines Ausbringungsprojekts das entsprechende Produkt auf den zugehörigen Systemen wieder deinstallieren möchten, wählen Sie in der Liste **Aktion** die Option **Deinstallieren** aus.

In der folgenden Tabelle werden die beiden Methoden zur Ausbringung von Produkten, d. h. einzelne Client-Task-Objekte und Produktausbringungsprojekte, miteinander verglichen.

Tabelle 12-1 Vergleich der Methoden zur Produktausbringung

Client-Task-Objekte	Vergleich der Funktionen	Produktausbringungsprojekt
Name und Beschreibung	Identisch	Name und Beschreibung
Erfassung von auszubringender Produkt-Software	Identisch	Erfassung von auszubringender Produkt-Software
Verwendung von Tags zur Auswahl von Zielsystemen	Verbessert in Produktausbringungsprojekten	Auswahl während der Ausbringung: • **Beliebig viele** – Bei Ausbringungen vom Typ **Beliebig viele** werden Systemstrukturgruppen oder Tags verwendet. Dadurch können Sie Systeme in bestimmte Gruppen verschieben oder Systemen bestimmte Tags zuweisen, sodass die Ausbringung dann auf den entsprechenden Systemen durchgeführt wird. • **Festgelegt** – Bei Ausbringungen vom Typ **Festgelegt** wird eine festgelegte bzw. definierte Auswahl an Systemen verwendet. Die Auswahl der Systeme erfolgt in der Systemstruktur oder mithilfe von Ausgabetabellen für Abfragen vom Typ **Verwaltete Systeme**.
Planung der Ausbringung	Ähnlich	Dank einer vereinfachten Ausbringungsplanung können Sie Ausbringungen entweder sofort oder zu einem geplanten Zeitpunkt ausführen.

Tabelle 12-1 Vergleich der Methoden zur Produktausbringung *(Fortsetzung)*

Client-Task-Objekte	Vergleich der Funktionen	Produktausbringungsprojekt
Nicht verfügbar	Neu in Produktausbringungsprojekten	Sie können den aktuellen Ausbringungsstatus überwachen (z. B. Ausbringungen, die geplant, aber noch nicht gestartet wurden, oder die gerade durchgeführt werden, angehalten oder abgeschlossen sind).
Nicht verfügbar	Neu in Produktausbringungsprojekten	Sie können einen Verlaufs-Snapshot zu Daten über die Anzahl der Systeme anzeigen, auf denen die Ausbringung erfolgt. Nur bei Ausbringungen vom Typ **Festgelegt**.
Nicht verfügbar	Neu in Produktausbringungsprojekten	Sie können den Status einzelner Systemausbringungen anzeigen (z. B. Installiert, Ausstehend oder Fehlgeschlagen).
Nicht verfügbar	Neu in Produktausbringungsprojekten	Sie können eine vorhandene Ausbringungszuweisung mithilfe folgender Optionen ändern: • Erstellen einer neuen Ausbringung zum Ändern einer vorhandenen • Bearbeiten • Duplizieren • Löschen • Anhalten einer Ausbringung • Fortsetzen einer Ausbringung • Deinstallieren

Erklärung der Seite "Produktausbringung"

Die Seite **Produktausbringung** ist die zentrale Stelle, an der Sie Produktausbringungsprojekte erstellen, überwachen und verwalten können.

Die Seite ist in zwei Hauptbereiche aufgeteilt (Bereich 1 und 2 im Bild unten), wobei der Bereich 2 noch einmal in fünf kleinere Bereiche unterteilt ist.

Abbildung 12-1 Erklärung der Seite "Produktausbringung"

Bei den beiden Hauptbereichen handelt es sich um:

1 Die **Ausbringungszusammenfassung** – Hier sind die Produktausbringungen aufgelistet, die Sie nach Typ und Status filtern können. Darüber hinaus erhalten Sie einen schnellen Überblick über deren Fortschritt. Wenn Sie auf eine Ausbringung klicken, werden deren Details im Bereich mit den Ausbringungsdetails angezeigt.



Ein Ausrufezeichen bedeutet, dass die Ausbringung entweder gerade deinstalliert wird oder dass das von der Ausbringung verwendete Paket verschoben oder gelöscht wurde.

2 Die **Ausbringungsdetails** – Hier werden die Einzelheiten zu der ausgewählten Ausbringung aufgelistet. Dieser Bereich enthält folgende Unterbereiche:

2a **Statusmonitor** – Welche Fortschritts- und Statusinformationen im Einzelnen angezeigt werden, hängt vom Typ der Ausbringung und deren Status ab:

- Bei Ausbringungen für eine beliebige Anzahl an Systemen wird ein Kalender angezeigt, wenn die Ausbringung noch aussteht, oder ein Balkendiagramm, wenn die Ausbringung gerade durchgeführt wird.
- Bei Ausbringungen für eine festgelegte Auswahl an Systemen wird ein Kalender angezeigt, wenn die Ausbringung noch aussteht, ein Balkendiagramm, wenn **Aktuell** ausgewählt ist, bzw. ein Histogramm, wenn **Dauer** ausgewählt ist.

2b **Details** – In diesem Bereich werden Details zur Konfiguration und zum Status der Ausbringung angezeigt. Bei Bedarf können Sie auf **Task-Details anzeigen** klicken, um die Seite **Ausbringung bearbeiten** zu öffnen.

2c **Systemname** – Hier wird eine filterbare Liste der Zielsysteme angezeigt, die die Ausbringung erhalten. Welche Systeme hier angezeigt werden, richtet sich nach dem Typ der Ausbringung sowie danach, auf welche Weise die Systeme ausgewählt wurden (d. h. einzeln, per Tags, per Systemstrukturgruppen oder mithilfe von Abfragetabellen).



Wenn Sie auf **Systemaktionen** klicken, wird die gefilterte Liste der Systeme in einem Dialogfeld angezeigt, das weitere Details enthält und in dem Sie Aktionen (wie Aktualisierungen oder Reaktivierungen) an den Systemen durchführen können.

2d **Status** – Zeigt eine dreiteilige Statusleiste an, die den Fortschritt der Ausbringung und deren Status angibt.

2e **Tags** – Hier werden die den Systemen zugeordneten Tags angezeigt.

Anzeigen von Audit-Protokollen zu Produktausbringungen

In den Audit-Protokolle der Ausbringungsprojekte sind alle Produktausbringungen aufgezeichnet, die über die Konsole mithilfe der Funktion zur Produktausbringung durchgeführt wurden.

Diese Audit-Protokolleinträge werden auf der Seite **Produktausbringung** im Bereich mit den Ausbringungsdetails in einer sortierbaren Tabelle sowie auf der Seite **Audit-Protokoll** angezeigt, die Protokolleinträge von allen überwachbaren Benutzeraktionen enthält. Mithilfe dieser Protokolle können Sie Produktausbringungen überwachen, erstellen, bearbeiten, duplizieren, löschen und deinstallieren. Klicken Sie auf einen Protokolleintrag, um dessen Details anzuzeigen.

Ausbringen von Produkten mithilfe eines Produktausbringungsprojekts

Wenn Sie Sicherheitsprodukte mithilfe eines Produktausbringungsprojekts auf verwalteten Systemen ausbringen, können Sie die auszubringenden Produkte sowie die Zielsysteme ganz leicht auswählen und die Ausbringung einfach planen.

Vorgehensweise

Definitionen zu Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

1. Klicken Sie auf **Menü** | **Software** | **Produktausbringung**.
2. Klicken Sie auf **Neue Ausbringung**, um die **Neue Ausbringung** zu öffnen und ein neues Projekt zu starten.
3. Geben Sie **Name** und **Beschreibung** für diese Ausbringung ein. Nach dem Speichern der Ausbringung wird dieser Name auf der Seite **Ausbringung** angezeigt.

4 Wählen Sie den Ausbringungstyp aus:

   - **Beliebig viele** – Die Systeme, die diese Ausbringung erhalten, werden mithilfe von Systemstrukturgruppen oder Tags konfiguriert. Dadurch können Sie im Laufe der Zeit ändern, welche Systeme eine Ausbringung erhalten, indem Sie die gewünschten Systeme zu den jeweiligen Gruppen oder Tags hinzufügen bzw. daraus entfernen.
   - **Festgelegt** – Hierbei wird eine feste bzw. definierte Auswahl an Systemen verwendet, die die Ausbringung erhalten sollen. Die Auswahl der Systeme erfolgt in der Systemstruktur oder mithilfe von Ausgabetabellen für Abfragen vom Typ **Verwaltete Systeme**.

5 Wählen Sie zum Festlegen der auszubringenden Software ein Produkt in der Liste **Paket** aus. Klicken Sie zum Hinzufügen oder Entfernen von Paketen auf **+** bzw. -.



Damit Software ausgebracht werden kann, muss sie im Master-Repository eingecheckt sein. Die Felder **Sprache** und **Zweig** werden anhand der im Master-Repository angegebenen Informationen zu Sprache und Speicherort automatisch ausgefüllt.

6 Im Textfeld **Befehlszeile** können Sie Optionen für befehlszeilengestützte Installationen angeben. Informationen über Befehlszeilenoptionen finden Sie in der Produktdokumentation der jeweiligen auszubringenden Software.

7 Klicken Sie im Dialogfeld **Systemauswahl** im Abschnitt **Systeme auswählen** auf **Systeme auswählen**.

   Das Dialogfeld **Systemauswahl** ist ein Filter, mit dem Sie Gruppen in der Systemstruktur, Tags oder eine Untermenge gruppierter und/oder mit Tags gekennzeichneter Systeme auswählen können. Die auf den einzelnen Registerkarten dieses Dialogfelds ausgewählten Elemente werden miteinander verbunden, um den kompletten Satz an Zielsystemen für die Ausbringung zu filtern.

   Wenn Ihre Systemstruktur beispielsweise eine "Gruppe A" enthält, in der sich sowohl Server als auch Workstations befinden, können Sie die gesamte Gruppe, nur die Server oder Workstations (wenn diese mit den entsprechenden Tags gekennzeichnet sind) oder eine Untermenge der in "Gruppe A" befindlichen Systemtypen herausfiltern.



Bei festgelegten Ausbringungen ist die Zahl der Systeme, die eine Ausbringung erhalten, auf maximal 500 beschränkt.

   Konfigurieren Sie bei Bedarf folgende Optionen:

   - **Bei jeder Richtlinienerzwingung ausführen (nur Windows)**
   - **Aufschieben der Ausbringung durch Endbenutzer zulassen (nur Windows)**
   - **Maximal zulässige Anzahl von Aufschubvorgängen**
   - **Option zum Aufschieben läuft ab nach**
   - **Diesen Text anzeigen**

8 Wählen Sie eine Startzeit oder einen Plan für Ihre Ausbringung aus:

   - **Sofort ausführen** – Startet den Ausbringungs-Task während des nächsten ASKIs.
   - **Einmal** – Öffnet den Planer, in dem Sie das Startdatum, die Uhrzeit und ein Zufallsintervall konfigurieren können.

9 Klicken Sie nach Abschluss aller Einstellungen oben auf der Seite auf **Speichern**. Die Seite **Produktausbringung** wird geöffnet, auf der Ihr neues Projekt zur Liste der Ausbringungen hinzugefügt ist.

Nachdem Sie ein Ausbringungsprojekt erstellt haben, wird automatisch ein Client-Task mit den Ausbringungseinstellungen erstellt.

Überwachen und Bearbeiten von Ausbringungsprojekten

Auf der Seite **Produktausbringung** können Sie Ausbringungsprojekte erstellen, überwachen und ändern.

In der folgenden Anleitung wird in den ersten Schritten beschrieben, wie Sie ein vorhandenes Ausbringungsprojekt mithilfe der Benutzeroberfläche auswählen und überwachen können, während in den letzten Schritten erläutert wird, wie Sie dieses Ausbringungsprojekt durch Auswahl von **Aktionen** ändern können.

Vorgehensweise

Definitionen zu Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

1. Klicken Sie auf **Menü | Software | Produktausbringung**. Die Seite **Produktausbringung** wird angezeigt.
2. Filtern Sie die Liste der Ausbringungsprojekte nach einer oder beiden der folgenden Optionen:
   - **Typ** – Filtert die anzuzeigenden Ausbringungen nach **Alle**, **Beliebig viele** oder **Festgelegt**.
   - **Status** – Filtert die anzuzeigenden Ausbringungen nach **Alle**, **Fertig gestellt**, **Wird ausgeführt**, **Ausstehend**, **Aktiv** oder **Angehalten**.
3. Wenn Sie links auf der Seite auf eine Ausbringung in der Liste klicken, werden rechts die Details zu dieser Ausbringung angezeigt.
4. Im Abschnitt **Fortschritt** der Detailanzeige können Sie Folgendes anzeigen:
   - Einen Kalender mit dem Startdatum für ausstehende Ausbringungen auf beliebig vielen oder auf einer festgelegten Auswahl von Systemen.
   - Ein Histogramm mit Systemen und der Zeitdauer bis zum Abschluss für Ausbringungen auf einer festgelegten Auswahl von Systemen.
   - Eine Statusleiste, die den Fortschritt von Systemausbringungen und -deinstallationen anzeigt.
5. Klicken Sie auf **Aktionen**, und wählen Sie eine der folgenden Optionen aus, um eine Ausbringung zu ändern:
   - **Bearbeiten**
   - **Löschen**
   - **Duplizieren**
   - **Als fertig gestellt kennzeichnen**
   - **Fortsetzen**
   - **Anhalten**
   - **Deinstallieren**
6. Klicken Sie im Detailbereich auf **Task-Details anzeigen**, um die Seite **Ausbringung bearbeiten** zu öffnen, auf der Sie die Einstellungen für die Ausbringung anzeigen und ändern können.
7. Klicken Sie in der Tabelle **Systeme** auf eine der folgenden Optionen in der Liste **Filter**, um den Typ der angezeigten Systeme zu ändern:

   Welche Optionen in der Liste aufgeführt sind, hängt vom aktuellen Status der Ausbringung ab.

   - Bei einer Deinstallation sind die folgenden Filter verfügbar: **Alle**, **Entfernte Pakete**, **Ausstehend** und **Fehlgeschlagen**.
   - Bei allen anderen Aktionen sind die folgenden Filter verfügbar: **Alle**, **Installation erfolgreich**, **Ausstehend** und **Fehlgeschlagen**.

8 In der Tabelle **Systeme** können Sie folgende Aktionen durchführen:

- In der Spalte **Status** können Sie den Status der aufgelisteten Zielsysteme überprüfen. Der Fortschritt der Ausbringung wird in einer dreiteiligen Statusleiste angezeigt.
- In der Spalte **Tags** können Sie die den einzelnen Zielsystemen zugeordneten Tags überprüfen.
- Wenn Sie auf **Systemaktionen** klicken, können Sie die Liste der Systeme auf einer neuen Seite anzeigen, auf der Sie an den ausgewählten Systemen systemspezifische Aktionen durchführen können.

13 Richtlinienverwaltung

Mithilfe von Richtlinien wird sichergestellt, dass die Funktionen eines Produkts auf verwalteten Systemen korrekt konfiguriert sind.

Das Verwalten von Produkten von einer zentralen Stelle aus ist eine Hauptfunktion von ePolicy Orchestrator. Erreichen können Sie dies u. a., indem Sie Produktrichtlinien anwenden und erzwingen. Richtlinien stellen sicher, dass die Funktionen von Produkten ordnungsgemäß konfiguriert sind, während Client-Tasks die geplanten Aktionen darstellen, die auf den verwalteten Systemen ausgeführt werden, auf denen sich Client-seitige Software befindet.

Inhalt

Richtlinien und Richtlinienerzwingung

Eine *Richtlinie* ist eine Sammlung von Einstellungen, die Sie erstellen, konfigurieren und dann erzwingen. Mit Richtlinien können Sie gewährleisten, dass die verwaltete Sicherheits-Software nach Ihren Anforderungen konfiguriert ist und funktioniert.

Einige Richtlinieneinstellungen sind mit den Einstellungen identisch, die Sie in der Benutzeroberfläche des auf dem verwalteten System installierten Produkts konfigurieren. Andere Richtlinieneinstellungen sind das primäre Tool für die Konfiguration des Produkts oder der Komponente. Mit der ePolicy Orchestrator-Konsole können Sie die Richtlinieneinstellungen für alle Produkte und Systeme zentral konfigurieren.

Richtlinienkategorien

Die Richtlinieneinstellungen für die meisten Produkte sind nach *Kategorien* zusammengefasst. Jede Richtlinienkategorie bezieht sich auf eine spezielle Teilgruppe von Richtlinieneinstellungen. Richtlinien werden nach Kategorien erstellt. Auf der Seite **Richtlinienkatalog** werden Richtlinien nach dem Produkt und der Kategorie angezeigt. Wenn Sie eine vorhandene Richtlinie öffnen oder eine neue Richtlinie erstellen, werden die Richtlinieneinstellungen in Registerkarten organisiert.

Wo werden Richtlinien angezeigt?

Klicken Sie zum Anzeigen aller Richtlinien, die zu den einzelnen Richtlinienkategorien erstellt wurden, auf **Menü** | **Richtlinie** | **Richtlinienkatalog**, und wählen Sie dann in den Dropdown-Listen ein **Produkt** und eine **Kategorie** aus. Auf der Seite **Richtlinienkatalog** werden dem Benutzer nur Richtlinien der Produkte angezeigt, für die der Benutzer über Berechtigungen verfügt.

Wenn Sie wissen möchten, welche Richtlinien pro Produkt auf eine bestimmte Gruppe der Systemstruktur angewendet werden, klicken Sie auf **Menü** | **Systeme** | **Systemstruktur** | **Zugewiesene Richtlinien**, wählen Sie die Gruppe aus, und wählen Sie dann in der Dropdown-Liste ein **Produkt** aus.



Für jede Kategorie gibt es eine Richtlinie "McAfee Default". Sie können diese Richtlinien zwar weder löschen, bearbeiten, exportieren noch umbenennen, Sie können sie jedoch kopieren und anschließend bearbeiten.

Festlegen der Richtlinienerzwingung

Sie können für jedes verwaltete Produkt oder jede verwaltete Komponente festlegen, ob der Agent sämtliche oder keine der Richtlinienbestimmungen für dieses Produkt oder diese Komponente erzwingt.

Auf der Seite **Zugewiesene Richtlinien** können Sie auswählen, ob Richtlinien für Produkte oder Komponenten bei der ausgewählten Gruppe erzwungen werden sollen.

Auf der Seite **Richtlinienkatalog** können Sie Richtlinienzuweisungen anzeigen und sehen, wo sie angewendet und ob sie erzwungen werden. Darüber hinaus können Sie die Richtlinienerzwingung sperren, um Änderungen an der Erzwingung unterhalb des gesperrten Knotens zu verhindern.



Wenn die Richtlinienerzwingung deaktiviert ist, erhalten in der angegebenen Gruppe befindliche Systeme während der Agent-zu-Server-Kommunikation keine aktualisierten Sitelists. Dies kann dazu führen, dass diese verwalteten Systeme nicht wie erwartet funktionieren. Wenn Sie zum Beispiel verwaltete Systeme so konfigurieren, dass sie mit der Agentensteuerung A kommunizieren sollen, die Richtlinienerzwingung jedoch deaktiviert ist, erhalten die verwalteten Systeme die neue Sitelist mit dieser Information nicht und melden sich daher bei einer anderen Agentensteuerung, die in einer abgelaufenen Sitelist aufgeführt ist.

Wann werden Richtlinien erzwungen?

Wenn Sie Richtlinieneinstellungen neu konfigurieren, werden die neuen Einstellungen bei der nächsten Agent-zu-Server-Kommunikation an die verwalteten Systeme übermittelt und dort erzwungen. Die Häufigkeit, in der diese Kommunikation erfolgt, wird von der Einstellung für das **Agent-zu-Server-Kommunikationsintervall** (ASKI) auf der Registerkarte **Allgemein** der McAfee Agent-Richtlinienseiten oder durch die Planung des McAfee Agent-Reaktivierungs-Tasks bestimmt (je nachdem, wie Sie die Agent-zu-Server-Kommunikation implementieren). Standardmäßig ist dieses Intervall auf einen Wert von 60 Minuten eingestellt.

Sobald die Richtlinieneinstellungen auf dem verwalteten System wirksam sind, setzt der Agent die Erzwingung der Richtlinieneinstellungen innerhalb eines regulären Intervalls lokal fort. Dieses Erzwingungsintervall wird durch die Einstellung **Richtlinienerzwingungsintervall** auf der Registerkarte **Allgemein** der **McAfee Agent**-Richtlinienseiten bestimmt. Standardmäßig ist dieses Intervall auf einen Wert von 5 Minuten eingestellt.

Richtlinieneinstellungen für McAfee-Produkte werden im Richtlinienerzwingungsintervall sofort und – wenn Richtlinieneinstellungen geändert wurden – bei jeder Agent-zu-Server-Kommunikation erzwungen.

Exportieren und Importieren von Richtlinien

Wenn Sie mehrere Server haben, können Sie Richtlinien zwischen diesen über XML-Dateien exportieren und importieren. Auf diese Weise müssen Sie eine Richtlinie nur einmal erstellen.

Sie können einzelne oder alle Richtlinien für ein bestimmtes Produkt exportieren und importieren.

Sie können diese Funktion auch dazu verwenden, um Sicherungskopien von Richtlinien zu erstellen, wenn Sie den Server neu installieren müssen.

Richtlinienfreigabe

Eine andere Möglichkeit zum Übertragen von Richtlinien zwischen Servern ist die Richtlinienfreigabe. Durch Freigeben von Richtlinien können Sie Richtlinien auf einem Server verwalten und diese dann über die McAfee ePO-Konsole auf vielen anderen Servern verwenden. Weitere Informationen dazu finden Sie unter *Freigeben von Richtlinien zwischen McAfee ePO-Servern*.

Richtlinienanwendung

Richtlinien werden auf jedes System durch *Vererbung* oder *Zuweisung* angewendet.

Vererbung

Die Richtlinienvererbung bestimmt, ob die Richtlinieneinstellungen und Client-Tasks für eine Gruppe oder ein System von dessen übergeordnetem Element übernommen werden. In der Standardeinstellung ist die Vererbung für die gesamte Systemstruktur aktiviert.

Wenn Sie diese Vererbung unterbrechen, indem Sie an einer bestimmten Stelle in der Systemstruktur eine neue Richtlinie zuweisen, wird diese Richtlinie von allen untergeordneten Gruppen und Systemen geerbt, für die festgelegt ist, dass sie die Richtlinie von diesem Zuweisungspunkt erben.

Zuweisung

Sie können eine Richtlinie im Richtlinienkatalog beliebigen Gruppen oder Systemen zuweisen (vorausgesetzt, Sie besitzen die entsprechenden Berechtigungen). Mittels Zuweisung können Sie Richtlinieneinstellungen für einen bestimmten Zweck einmal definieren und die Richtlinie dann auf mehrere Stellen anwenden.

Wenn Sie einer bestimmten Gruppe der Systemstruktur eine neue Richtlinie zuweisen, wird diese Richtlinie von allen untergeordneten Gruppen und Systemen geerbt, für die festgelegt ist, dass sie die Richtlinie von diesem Zuweisungspunkt erben.

Sperren von Zuweisungen

Sie können die Zuweisung einer Richtlinie für Gruppen oder Systeme sperren (vorausgesetzt, Sie besitzen die entsprechenden Berechtigungen). Durch das Sperren von Zuweisungen wird verhindert, dass:

- Benutzer mit entsprechenden Berechtigungen auf derselben Ebene der Systemstruktur versehentlich eine Richtlinie austauschen.
- Benutzer mit niedrigeren Berechtigungen (oder denselben Berechtigungen, aber auf einer niedrigeren Ebene der Systemstruktur) die Richtlinie austauschen.

Die Sperrung von Zuweisungen wird mit den Richtlinieneinstellungen vererbt.

Das Sperren von Zuweisungen ist nützlich, wenn Sie eine bestimmte Richtlinie an der Spitze der Systemstruktur zuweisen und dabei sicherstellen möchten, dass diese Richtlinie nicht an anderer Stelle in der Systemstruktur durch Benutzer ausgetauscht wird.

Das Sperren von Zuweisungen sperrt nur die Zuweisung der Richtlinie, verhindert aber nicht, dass der Besitzer der Richtlinie Änderungen an den Einstellungen vornehmen kann. Wenn Sie eine Richtlinienzuweisung sperren möchten, sollten Sie daher sicherstellen, dass Sie der Besitzer der Richtlinie sind.

Richtlinienbesitz

Alle Richtlinien für Produkte und Funktionen, für die Sie Berechtigungen besitzen, sind über die Seite **Richtlinienkatalog** verfügbar. Damit Benutzer keine Richtlinien anderer Benutzer bearbeiten können, ist jeder Richtlinie ein Besitzer zugewiesen. Dabei handelt es sich um den Benutzer, der sie erstellt hat.

Der Besitz einer Richtlinie gewährleistet, dass eine Richtlinie von niemandem außer dem Administrator oder dem Benutzer, der die Richtlinie erstellt hat, geändert oder gelöscht werden kann. Jeder Benutzer mit den entsprechenden Berechtigungen kann Richtlinien im **Richtlinienkatalog** zuweisen, aber nur der Besitzer oder ein Administrator kann sie ändern.

Wenn Sie verwalteten Systemen eine Richtlinie zuweisen, deren Besitzer Sie nicht sind, müssen Sie Folgendes beachten: Wird diese benannte Richtlinie durch den Besitzer geändert, werden diese Änderungen auf allen Systemen wirksam, denen diese Richtlinie zugewiesen ist. Daher sollten Sie, wenn Sie eine Richtlinie verwenden möchten, die sich im Besitz eines anderen Benutzers befindet, zunächst ein Duplikat dieser Richtlinie erstellen und dann dieses Duplikat an den gewünschten Stellen zuweisen. Auf diese Weise werden Sie Besitzer der zugewiesenen Richtlinie.



Sie können mehrere Benutzer, die keine Administratoren sind, als Besitzer für eine einzige Richtlinie festlegen.

Erstellen und Verwalten von Richtlinien

Sie können auf der Seite **Richtlinienkatalog** Richtlinien erstellen und verwalten.

Aufgaben

- *Erstellen einer Richtlinie auf der Seite "Richtlinienkatalog"* auf Seite 182
  Sie können im Richtlinienkatalog eine neue Richtlinie erstellen.
- *Verwalten einer vorhandenen Richtlinie auf der Seite "Richtlinienkatalog"* auf Seite 183
  Eine erstellte Richtlinie können Sie bearbeiten, duplizieren, umbenennen und löschen.
- *Steuern der Sichtbarkeit von Richtlinien für nicht unterstützte Produkte* auf Seite 184
  Nach einer gewissen Betriebszeit des ePolicy Orchestrator-Servers oder einer Aktualisierung von einer älteren Version der Software befinden sich auf dem Server möglicherweise einige nicht unterstützte Produkte. Im **Richtlinienkatalog** können Sie steuern, ob die zu diesen Produkten gehörenden Richtlinien angezeigt werden.

Erstellen einer Richtlinie auf der Seite "Richtlinienkatalog"

Sie können im Richtlinienkatalog eine neue Richtlinie erstellen.

Standardmäßig sind hier erstellte Richtlinien keinen Gruppen oder Systemen zugewiesen. Wenn Sie hier eine Richtlinie erstellen, fügen Sie eine benutzerdefinierte Richtlinie zum Richtlinienkatalog hinzu. Sie können Richtlinien vor oder nach dem Ausbringen eines Produkts erstellen.

Definitionen zu Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

Vorgehensweise

1. Klicken Sie auf **Menü | Richtlinie | Richtlinienkatalog**, und wählen Sie dann in den Dropdown-Listen das **Produkt** und die **Kategorie** aus.

   Alle für die ausgewählte Kategorie erstellten Richtlinien werden im Detailbereich angezeigt.

2. Klicken Sie auf **Aktionen | Neue Richtlinie**.

   Das Dialogfeld **Neue Richtlinie** wird angezeigt.

3. Wählen Sie in der Dropdown-Liste **Richtlinie auf Grundlage dieser vorhandenen Richtlinie erstellen** die Richtlinie aus, die Sie duplizieren möchten.

4. Geben Sie einen Namen für die neue Richtlinie ein, und klicken Sie auf **OK**.

   Der Assistent **Richtlinieneinstellungen** wird angezeigt.

5. Bearbeiten Sie die Richtlinieneinstellungen auf den einzelnen Registerkarten nach Bedarf.

6. Klicken Sie auf **Speichern**.

Verwalten einer vorhandenen Richtlinie auf der Seite "Richtlinienkatalog"

Eine erstellte Richtlinie können Sie bearbeiten, duplizieren, umbenennen und löschen.

Vorgehensweise

Definitionen zu Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

1. Klicken Sie zum Auswählen einer vorhandenen Richtlinie auf **Menü | Richtlinie | Richtlinienkatalog**, und wählen Sie dann in den Dropdown-Listen das **Produkt** und die **Kategorie** aus.

   Alle für die ausgewählte Kategorie erstellten Richtlinien werden im Detailbereich angezeigt.

2. Wählen Sie in den Listen das Produkt und die Kategorie für die zu ändernde Richtlinie aus.

   Alle für die ausgewählte Kategorie erstellten Richtlinien werden im Detailbereich angezeigt.

3. Wählen Sie eine der folgenden Aktionen aus.

Aktion	Vorgehensweise
Bearbeiten von Richtlinieneinstellungen	1 Suchen Sie die zu bearbeitende Richtlinie, und klicken Sie dann auf den Richtliniennamen. 2 Bearbeiten Sie die Einstellungen nach Bedarf, und klicken Sie dann auf **Speichern**.
Duplizieren einer Richtlinie	1 Suchen Sie die Richtlinie, die Sie duplizieren möchten, und klicken Sie dann in der Zeile der Richtlinie auf **Duplizieren**. Das Dialogfeld **Vorhandene Richtlinie duplizieren** wird angezeigt. 2 Geben Sie den Namen für die neue Richtlinie in das Feld ein, und klicken Sie auf **OK** Die neue Richtlinie wird auf der Seite **Richtlinienkatalog** angezeigt. 3 Klicken Sie auf die neue Richtlinie in der Liste. 4 Bearbeiten Sie die Einstellungen nach Bedarf, und klicken Sie dann auf **Speichern**. Die duplizierte Richtlinie wird mit ihrem neuen Namen und ihren neuen Einstellungen im Detailbereich angezeigt.
Umbenennen einer Richtlinie	1 Suchen Sie die Richtlinie, die Sie umbenennen möchten, und klicken Sie dann in der Zeile der gewünschten Richtlinie auf **Umbenennen**. Das Dialogfeld **Richtlinie umbenennen** wird angezeigt. 2 Geben Sie einen neuen Namen für die vorhandene Richtlinie ein, und klicken Sie dann auf **OK**. Die umbenannte Richtlinie wird im Detailbereich angezeigt.
Löschen einer Richtlinie	1 Suchen Sie die gewünschte Richtlinie, und klicken Sie dann in der Zeile der Richtlinie auf **Löschen**. 2 Klicken Sie auf **OK**, wenn Sie dazu aufgefordert werden. Die gelöschte Richtlinie wird aus dem Detailbereich entfernt.

Steuern der Sichtbarkeit von Richtlinien für nicht unterstützte Produkte

Nach einer gewissen Betriebszeit des ePolicy Orchestrator-Servers oder einer Aktualisierung von einer älteren Version der Software befinden sich auf dem Server möglicherweise einige nicht unterstützte Produkte. Im **Richtlinienkatalog** können Sie steuern, ob die zu diesen Produkten gehörenden Richtlinien angezeigt werden.

Wenn auf dem Server nicht unterstützte Produkte eingecheckt wurden, können Sie festlegen, ob deren Richtlinien ein- oder ausgeblendet werden sollen.

Vorgehensweise

Definitionen zu Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

1. Klicken Sie auf **Menü** | **Konfiguration** | **Server-Einstellungen**, wählen Sie in der Liste **Einstellungskategorien** den Eintrag **Richtlinienwartung** aus, und klicken Sie dann auf **Bearbeiten**.
2. Geben Sie an, ob Richtlinien für nicht unterstützte Produkte ein- oder ausgeblendet werden sollen, löschen Sie wahlweise nicht unterstützte Produkte, und klicken Sie dann auf **Speichern**.

Erstmaliges Konfigurieren von Richtlinien

Gehen Sie wie nachfolgend allgemein beschrieben vor, wenn Sie Ihre Richtlinien zum ersten Mal konfigurieren.

1. Planen Sie Produktrichtlinien für die Segmente Ihrer Systemstruktur.
2. Erstellen Sie Richtlinien für Gruppen und Systeme, und weisen Sie sie diesen zu.

Verwalten von Richtlinien

Sie können Richtlinien in Ihrer Umgebung zuweisen und verwalten.

Aufgaben

- *Konfigurieren von Agenten-Richtlinien zum Verwenden eines verteilten Repositorys* auf Seite 186
  Sie können anpassen, wie Agenten verteilte Repositories zur Minimierung der Bandbreitennutzung auswählen.
- *Ändern der Besitzer einer Richtlinie* auf Seite 186
  Standardmäßig wird der Ersteller einer Richtlinie auch als deren Besitzer festgelegt. Mithilfe des folgenden Tasks – der nur von Administratoren durchgeführt werden kann – können Sie den Besitzer einer Richtlinie ändern.
- *Verschieben von Richtlinien zwischen McAfee ePO-Servern* auf Seite 187
  Um Richtlinien zwischen McAfee ePO-Servern zu verschieben, müssen Sie die Richtlinie auf der Seite **Richtlinienkatalog** des Quell-Servers in eine XML-Datei exportieren und dann in die Seite **Richtlinienkatalog** auf dem Ziel-Server importieren.
- *Zuweisen einer Richtlinie zu einer Systemstrukturgruppe* auf Seite 188
  Sie können einer bestimmten Gruppe der Systemstruktur eine Richtlinie zuweisen. Diese Richtlinienzuweisung können Sie vor oder nach der Produktausbringung vornehmen.
- *Zuweisen einer Richtlinie zu einem verwalteten System* auf Seite 188
  Sie können einem bestimmten verwalteten System eine Richtlinie zuweisen. Diese Richtlinienzuweisung können Sie vor oder nach der Produktausbringung vornehmen.
- *Zuweisen einer Richtlinie zu Systemen in einer Systemstrukturgruppe* auf Seite 189
  Sie können mehreren verwalteten Systemen innerhalb einer Gruppe eine Richtlinie zuweisen. Diese Richtlinienzuweisung können Sie vor oder nach der Produktausbringung vornehmen.
- *Erzwingen von Richtlinien für ein Produkt in einer Systemstrukturgruppe* auf Seite 190
  Sie können die Richtlinienerzwingung für ein Produkt in einer Gruppe aktivieren oder deaktivieren. Die Richtlinienerzwingung ist standardmäßig aktiviert und wird in der Systemstruktur vererbt.
- *Erzwingen von Richtlinien für ein Produkt auf einem System* auf Seite 190
  Sie können die Richtlinienerzwingung für ein Produkt auf einem verwalteten System aktivieren oder deaktivieren. Die Richtlinienerzwingung ist standardmäßig aktiviert und wird in der Systemstruktur vererbt.
- *Kopieren von Richtlinienzuweisungen* auf Seite 191
  Sie können Richtlinienzuweisungen aus einer Gruppe oder einem System in eine andere Gruppe bzw. ein anderes System kopieren. Das ist eine einfache Methode, um mehrere Zuweisungen zwischen Gruppen und Systemen an unterschiedlichen Stellen der Systemstruktur freizugeben.

Konfigurieren von Agenten-Richtlinien zum Verwenden eines verteilten Repositorys

Sie können anpassen, wie Agenten verteilte Repositories zur Minimierung der Bandbreitennutzung auswählen.

Vorgehensweise

Definitionen zu Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

1. Klicken Sie auf **Menü** | **Richtlinie** | **Richtlinienkatalog**, und wählen Sie dann in der Dropdown-Liste **Produkt** den Eintrag **McAfee Agent** und in der Dropdown-Liste **Kategorie** den Eintrag **Repository** aus.
2. Klicken Sie auf die erforderliche vorhandene Agenten-Richtlinie.
3. Wählen Sie die Registerkarte **Repositories** aus.
4. Wählen Sie unter **Repository-Listenauswahl** entweder **Diese Repository-Liste verwenden** oder **Andere Repository-Liste verwenden** aus.
5. Geben Sie unter **Repository auswählen nach** die Methode an, die zum Sortieren von Repositories verwendet werden soll:
    - **Ping-Zeit** – Sendet einen ICMP-Ping an die (nach dem Subnetzwert) nächstgelegenen fünf Repositories und sortiert diese nach der Reaktionszeit.
    - **Subnetzentfernung** – Vergleicht die IP-Adressen von Client-Systemen und sämtlichen Repositories und sortiert Repositories danach, wie genau die Bits übereinstimmen. Je mehr die IP-Adressen übereinstimmen, desto höher wird das Repository in der Liste eingestuft.

      Bei Bedarf können Sie die **Maximale Anzahl der Hops** festlegen.
    - **Reihenfolge in der Repository-Liste verwenden** – Wählt Repositories auf Grundlage ihrer Reihenfolge in der Liste aus.
6. In der **Repository-Liste** können Sie Repositories deaktivieren, indem Sie im Feld **Aktionen** des Repositories, das Sie deaktivieren möchten, auf **Deaktivieren** klicken.
7. Klicken Sie in der **Repository-Liste** auf **Zum Anfang** oder **Zum Ende**, um die Reihenfolge festzulegen, in der verteilte Repositories von Client-Systemen ausgewählt werden sollen.
8. Klicken Sie abschließend auf **Speichern**.

Ändern der Besitzer einer Richtlinie

Standardmäßig wird der Ersteller einer Richtlinie auch als deren Besitzer festgelegt. Mithilfe des folgenden Tasks – der nur von Administratoren durchgeführt werden kann – können Sie den Besitzer einer Richtlinie ändern.

Vorgehensweise

Definitionen zu Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

1. Klicken Sie auf **Menü** | **Richtlinie** | **Richtlinienkatalog**, und wählen Sie dann das **Produkt** und die **Kategorie** aus.

   Alle für die ausgewählte Kategorie erstellten Richtlinien werden im Detailbereich angezeigt.
2. Suchen Sie die gewünschte Richtlinie, und klicken Sie dann auf den Besitzer der Richtlinie.

   Die Seite **Richtlinienbesitz** wird angezeigt.
3. Wählen Sie in der Liste die gewünschten Besitzer der Richtlinie aus, und klicken Sie anschließend auf **OK**.

Verschieben von Richtlinien zwischen McAfee ePO-Servern

Um Richtlinien zwischen McAfee ePO-Servern zu verschieben, müssen Sie die Richtlinie auf der Seite **Richtlinienkatalog** des Quell-Servers in eine XML-Datei exportieren und dann in die Seite **Richtlinienkatalog** auf dem Ziel-Server importieren.

Aufgaben

- *Exportieren einer einzelnen Richtlinie* auf Seite 187
  Sie können eine einzelne Richtlinie in eine XML-Datei exportieren und diese Datei dann verwenden, um die Richtlinie in einen anderen McAfee ePO-Server zu importieren oder um die Datei zur Sicherung der Richtlinie aufzubewahren.
- *Exportieren aller Richtlinien eines Produkts* auf Seite 187
  Gehen Sie wie in dieser Aufgabe beschrieben vor, um alle Richtlinien eines Produkts in eine XML-Datei zu exportieren. Mithilfe dieser Datei können Sie die Richtlinie auf einen anderen McAfee ePO-Server importieren oder eine Sicherung der Richtlinien aufbewahren.
- *Importieren von Richtlinien* auf Seite 188
  Sie können eine XML-Richtliniendatei importieren. Der Import verläuft immer gleich, unabhängig davon, ob Sie eine einzelne oder alle benannten Richtlinien exportiert haben.

Exportieren einer einzelnen Richtlinie

Sie können eine einzelne Richtlinie in eine XML-Datei exportieren und diese Datei dann verwenden, um die Richtlinie in einen anderen McAfee ePO-Server zu importieren oder um die Datei zur Sicherung der Richtlinie aufzubewahren.

Vorgehensweise

Definitionen zu Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

1. Klicken Sie auf **Menü | Richtlinie | Richtlinienkatalog**, und wählen Sie dann in den Dropdown-Listen das **Produkt** und die **Kategorie** aus.

   Alle für die ausgewählte Kategorie erstellten Richtlinien werden im Detailbereich angezeigt.
2. Suchen Sie die gewünschte Richtlinie, und klicken Sie dann neben der Richtlinie auf **Exportieren**.

   Die Seite **Exportieren** wird angezeigt.
3. Klicken Sie mit der rechten Maustaste auf den Link, um die Datei herunterzuladen und zu speichern.
4. Geben Sie einen Namen für die XML-Richtliniendatei ein, und speichern Sie sie.



Wenn Sie diese Datei auf einen anderen McAfee ePO-Server importieren möchten, müssen Sie sicherstellen, dass der ePolicy Orchestrator-Ziel-Server auf diesen Speicherort zugreifen kann.

Exportieren aller Richtlinien eines Produkts

Gehen Sie wie in dieser Aufgabe beschrieben vor, um alle Richtlinien eines Produkts in eine XML-Datei zu exportieren. Mithilfe dieser Datei können Sie die Richtlinie auf einen anderen McAfee ePO-Server importieren oder eine Sicherung der Richtlinien aufbewahren.

Vorgehensweise

Definitionen zu Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

1. Klicken Sie auf **Menü | Richtlinie | Richtlinienkatalog**, und wählen Sie dann das **Produkt** und die **Kategorie** aus.

   Alle für die ausgewählte Kategorie erstellten Richtlinien werden im Detailbereich angezeigt.

2 Klicken Sie neben **Produktrichtlinien** auf **Exportieren**. Die Seite **Exportieren** wird angezeigt.

3 Klicken Sie mit der rechten Maustaste auf den Link, um die Datei herunterzuladen und zu speichern.



Wenn Sie diese Datei auf einen anderen McAfee ePO-Server importieren möchten, müssen Sie sicherstellen, dass der ePolicy Orchestrator-Ziel-Server auf diesen Speicherort zugreifen kann.

Importieren von Richtlinien

Sie können eine XML-Richtliniendatei importieren. Der Import verläuft immer gleich, unabhängig davon, ob Sie eine einzelne oder alle benannten Richtlinien exportiert haben.

Vorgehensweise

Definitionen zu Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

1 Klicken Sie auf **Menü** | **Richtlinie** | **Richtlinienkatalog**, und klicken Sie dann neben **Produktrichtlinien** auf **Importieren**.

2 Suchen und wählen Sie die gewünschte XML-Richtliniendatei aus, und klicken Sie dann auf **OK**.

3 Wählen Sie die zu importierenden Richtlinien aus, und klicken Sie auf **OK**.

   Die Richtlinien werden zum Richtlinienkatalog hinzugefügt.

Zuweisen einer Richtlinie zu einer Systemstrukturgruppe

Sie können einer bestimmten Gruppe der Systemstruktur eine Richtlinie zuweisen. Diese Richtlinienzuweisung können Sie vor oder nach der Produktausbringung vornehmen.

Vorgehensweise

Definitionen zu Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

1 Klicken Sie auf **Menü** | **Systeme** | **Systemstruktur** | **Zugewiesene Richtlinien**, und wählen Sie dann in der Dropdown-Liste ein **Produkt** aus.

   Jede pro Kategorie zugewiesene Richtlinie wird im Detailbereich angezeigt.

2 Suchen Sie die gewünschte Richtlinienkategorie, und klicken Sie dann auf **Zuweisung bearbeiten**.

   Die Seite **Richtlinienzuweisung** wird angezeigt.

3 Wenn die Richtlinie geerbt wurde, wählen Sie neben **Geerbt von** die Option **Vererbung unterbrechen und ab hier Richtlinie und Einstellungen zuweisen** aus.

4 Wählen Sie in der Dropdown-Liste **Zugewiesene Richtlinie** die gewünschte Richtlinie aus.



An dieser Stelle können Sie auch die Einstellungen der ausgewählten Richtlinie bearbeiten oder eine Richtlinie erstellen.

5 Legen Sie fest, ob die Richtlinienvererbung gesperrt werden soll.

   Durch das Sperren der Richtlinienvererbung wird verhindert, dass Systemen, die diese Richtlinie erben, eine andere Richtlinie zugewiesen wird.

6 Klicken Sie auf **Speichern**.

Zuweisen einer Richtlinie zu einem verwalteten System

Sie können einem bestimmten verwalteten System eine Richtlinie zuweisen. Diese Richtlinienzuweisung können Sie vor oder nach der Produktausbringung vornehmen.

Vorgehensweise

Definitionen zu Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

1. Klicken Sie auf **Menü | Systeme | Systemstruktur | Systeme**, und wählen Sie dann in der Systemstruktur eine Gruppe aus.

   Alle Systeme, die sich in dieser Gruppe (aber nicht ihren Untergruppen) befinden, werden im Detailbereich angezeigt.

2. Wählen Sie ein System aus, und klicken Sie auf **Aktionen | Agent | Richtlinien auf einem einzelnen System ändern**.

   Die Seite **Richtlinienzuweisung** für dieses System wird angezeigt.

3. Wählen Sie ein Produkt aus.

   Die Kategorien der ausgewählten Produkte werden mit der dem System zugewiesenen Richtlinie aufgeführt.

4. Suchen Sie die gewünschte Richtlinienkategorie, und klicken Sie dann auf **Zuweisungen bearbeiten**.

5. Wenn die Richtlinie geerbt wurde, wählen Sie neben **Vererbt von** die Option **Vererbung unterbrechen und ab hier Richtlinie und Einstellungen zuweisen** aus.

6. Wählen Sie in der Dropdown-Liste **Zugewiesene Richtlinie** die gewünschte Richtlinie aus.

   An dieser Stelle können Sie auch die Einstellungen der ausgewählten Richtlinie bearbeiten oder eine Richtlinie erstellen.

7. Legen Sie fest, ob die Richtlinienvererbung gesperrt werden soll.

   Durch das Sperren der Richtlinienvererbung wird verhindert, dass Systemen, die diese Richtlinie erben, eine andere Richtlinie zugewiesen wird.

8. Klicken Sie auf **Speichern**.

Zuweisen einer Richtlinie zu Systemen in einer Systemstrukturgruppe

Sie können mehreren verwalteten Systemen innerhalb einer Gruppe eine Richtlinie zuweisen. Diese Richtlinienzuweisung können Sie vor oder nach der Produktausbringung vornehmen.

Vorgehensweise

Definitionen zu Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

1. Klicken Sie auf **Menü | Systeme | Systemstruktur | Systeme**, und wählen Sie dann in der Systemstruktur eine Gruppe aus.

   Alle Systeme, die sich in dieser Gruppe (aber nicht ihren Untergruppen) befinden, werden im Detailbereich angezeigt.

2. Wählen Sie die gewünschten Systeme aus, und klicken Sie dann auf **Aktionen | Agent | Richtlinie und Vererbung zuweisen**.

   Die Seite **Richtlinie zuweisen** wird angezeigt.

3. Wählen Sie das **Produkt**, die **Kategorie** und die **Richtlinie** in den entsprechenden Dropdown-Listen aus.

4. Aktivieren Sie **Vererbung zurücksetzen** oder **Vererbung unterbrechen**, und klicken Sie dann auf **Speichern**.

Erzwingen von Richtlinien für ein Produkt in einer Systemstrukturgruppe

Sie können die Richtlinienerzwingung für ein Produkt in einer Gruppe aktivieren oder deaktivieren. Die Richtlinienerzwingung ist standardmäßig aktiviert und wird in der Systemstruktur vererbt.

Vorgehensweise

Definitionen zu Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

1. Klicken Sie auf **Menü | Systeme | Systemstruktur | Zugewiesene Richtlinien**, und wählen Sie dann in der Systemstruktur die gewünschte Gruppe aus.
2. Wählen Sie das gewünschte **Produkt** aus, und klicken Sie dann auf den Link neben **Erzwingungsstatus**.

   Die Seite **Erzwingen für** wird angezeigt.
3. Wenn Sie den Erzwingungsstatus ändern möchten, müssen Sie zuerst **Vererbung unterbrechen und ab hier Richtlinie und Einstellungen zuweisen** auswählen.
4. Wählen Sie neben **Erzwingungsstatus** entsprechend **Wird erzwungen** oder **Wird nicht erzwungen** aus.
5. Legen Sie fest, ob die Richtlinienvererbung gesperrt werden soll.

   Durch das Sperren der Richtlinienvererbung wird verhindert, dass die Vererbung für Gruppen und Systeme unterbrochen wird, die diese Richtlinie erben.
6. Klicken Sie auf **Speichern**.

Erzwingen von Richtlinien für ein Produkt auf einem System

Sie können die Richtlinienerzwingung für ein Produkt auf einem verwalteten System aktivieren oder deaktivieren. Die Richtlinienerzwingung ist standardmäßig aktiviert und wird in der Systemstruktur vererbt.

Vorgehensweise

Definitionen zu Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

1. Klicken Sie auf **Menü | Systeme | Systemstruktur | Systeme**, und wählen Sie dann unter **Systemstruktur** die Gruppe aus, zu der das System gehört.

   Alle Systeme, die zu der ausgewählten Gruppe gehören, werden im Detailbereich angezeigt.
2. Wählen Sie das gewünschte System aus, und klicken Sie auf **Aktionen | Richtlinien auf einem einzelnen System ändern**.

   Die Seite **Richtlinienzuweisung** wird angezeigt.
3. Wählen Sie das gewünschte **Produkt** aus, und klicken Sie dann neben **Erzwingungsstatus** auf **Wird erzwungen**.

   Die Seite **Erzwingen für** wird angezeigt.
4. Wenn Sie den Erzwingungsstatus ändern möchten, müssen Sie zuerst **Vererbung unterbrechen und ab hier Richtlinie und Einstellungen zuweisen** auswählen.
5. Wählen Sie neben **Erzwingungsstatus** entsprechend **Wird erzwungen** oder **Wird nicht erzwungen** aus.
6. Klicken Sie auf **Speichern**.

Kopieren von Richtlinienzuweisungen

Sie können Richtlinienzuweisungen aus einer Gruppe oder einem System in eine andere Gruppe bzw. ein anderes System kopieren. Das ist eine einfache Methode, um mehrere Zuweisungen zwischen Gruppen und Systemen an unterschiedlichen Stellen der Systemstruktur freizugeben.

Aufgaben

- *Kopieren von Richtlinienzuweisungen aus einer Gruppe* auf Seite 191
  Sie können Richtlinienzuweisungen aus einer Gruppe in der Systemstruktur in eine andere kopieren.
- *Kopieren von Richtlinienzuweisungen aus einem System* auf Seite 191
  Sie können Richtlinienzuweisungen aus einem bestimmten System kopieren.
- *Einfügen von Richtlinienzuweisungen in eine Gruppe* auf Seite 191
  Nachdem Sie die Richtlinienzuweisungen aus einer Gruppe oder einem System kopiert haben, können Sie sie in eine Gruppe einfügen.
- *Einfügen von Richtlinienzuweisungen für ein bestimmtes System* auf Seite 192
  Nachdem Sie die Richtlinienzuweisungen aus einer Gruppe oder einem System kopiert haben, können Sie sie in ein bestimmtes System einfügen.

Kopieren von Richtlinienzuweisungen aus einer Gruppe

Sie können Richtlinienzuweisungen aus einer Gruppe in der Systemstruktur in eine andere kopieren.

Vorgehensweise

Definitionen zu Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

1. Klicken Sie auf **Menü** | **Systeme** | **Systemstruktur** | **Zugewiesene Richtlinien**, und wählen Sie dann in der Systemstruktur die gewünschte Gruppe aus.
2. Klicken Sie auf **Aktionen** | **Zuweisungen kopieren**.
3. Wählen Sie die Produkte oder Funktionen aus, für die Sie Richtlinienzuweisungen kopieren möchten, und klicken Sie dann auf **OK**.

Kopieren von Richtlinienzuweisungen aus einem System

Sie können Richtlinienzuweisungen aus einem bestimmten System kopieren.

Vorgehensweise

Definitionen zu Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

1. Klicken Sie auf **Menü** | **Systeme** | **Systemstruktur** | **Systeme**, und wählen Sie dann in der Systemstruktur die gewünschte Gruppe aus.

   Die Systeme, die zu der ausgewählten Gruppe gehören, werden im Detailbereich angezeigt.
2. Wählen Sie das gewünschte System aus, und klicken Sie auf **Aktionen** | **Agent** | **Richtlinien auf einem einzelnen System ändern**.
3. Klicken Sie auf **Aktionen** | **Richtlinienzuweisungen kopieren**, wählen Sie die gewünschten Produkte oder Funktionen aus, für die Sie Richtlinienzuweisungen kopieren möchten, und klicken Sie dann auf **OK**.

Einfügen von Richtlinienzuweisungen in eine Gruppe

Nachdem Sie die Richtlinienzuweisungen aus einer Gruppe oder einem System kopiert haben, können Sie sie in eine Gruppe einfügen.

Vorgehensweise

Definitionen zu Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

1. Klicken Sie auf **Menü** | **Systeme** | **Systemstruktur** | **Zugewiesene Richtlinien**, und wählen Sie dann in der Systemstruktur die gewünschte Gruppe aus.
2. Klicken Sie im Detailbereich auf **Aktionen**, und wählen Sie **Zuweisungen einfügen** aus.

   Wenn der Gruppe bereits für einige Kategorien Richtlinien zugewiesen sind, wird die Seite **Richtlinienzuweisungen außer Kraft setzen** angezeigt.

   Beim Einfügen von Richtlinienzuweisungen wird eine zusätzliche Richtlinie in der Liste angezeigt (Richtlinien und Tasks erzwingen). Diese Richtlinie steuert den Erzwingungsstatus anderer Richtlinien.

3. Wählen Sie aus, welche Richtlinienkategorien Sie durch die kopierten Richtlinien ersetzen möchten, und klicken Sie dann auf **OK**.

Einfügen von Richtlinienzuweisungen für ein bestimmtes System

Nachdem Sie die Richtlinienzuweisungen aus einer Gruppe oder einem System kopiert haben, können Sie sie in ein bestimmtes System einfügen.

Vorgehensweise

Definitionen zu Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

1. Klicken Sie auf **Menü** | **Systeme** | **Systemstruktur** | **Systeme**, und wählen Sie dann in der Systemstruktur die gewünschte Gruppe aus.

   Alle Systeme, die zu der ausgewählten Gruppe gehören, werden im Detailbereich angezeigt.

2. Wählen Sie das System aus, zu dem Sie Richtlinienzuweisungen einfügen möchten, und klicken Sie dann auf **Aktionen** | **Agent** | **Richtlinien auf einem einzelnen System ändern**.
3. Klicken Sie im Detailbereich auf **Aktionen** | **Zuweisungen einfügen**.

   Wenn dem System bereits für einige Kategorien Richtlinien zugewiesen sind, wird die Seite **Richtlinienzuweisungen außer Kraft setzen** angezeigt.

   Beim Einfügen von Richtlinienzuweisungen wird eine zusätzliche Richtlinie in der Liste angezeigt (Richtlinien und Tasks erzwingen). Diese Richtlinie steuert den Erzwingungsstatus anderer Richtlinien.

4. Bestätigen Sie das Ersetzen von Zuweisungen.

Richtlinienzuweisungsregeln

Durch Richtlinienzuweisungsregeln sinkt der Aufwand für das Verwalten einer Vielzahl von Richtlinien für einzelne Benutzer oder Systeme, die bestimmten Kriterien entsprechen, während für die gesamte Systemstruktur allgemeinere Richtlinien geführt werden.

Durch diese Abstufungen bei der Richtlinienzuweisung werden die Instanzen mit unterbrochener Vererbung in der Systemstruktur begrenzt, die erforderlich sind, um den Richtlinieneinstellungen gerecht zu werden, die für bestimmte Benutzer oder Systeme benötigt werden. Richtlinienzuweisungen können auf benutzerspezifischen oder systemspezifischen Kriterien basieren:

- *Benutzerbasierte Richtlinien* – Das sind Richtlinien, die mindestens ein benutzerspezifisches Kriterium enthalten. So können Sie zum Beispiel eine Richtlinienzuweisungsregel erstellen, die für alle Benutzer in der Entwicklungsabteilungsgruppe erzwungen wird. Anschließend können Sie eine andere Richtlinienzuweisungsregel für Mitglieder Ihrer IT-Abteilung erstellen, sodass sich diese bei jedem Computer im Netzwerk der Entwicklungsabteilung mit den Zugriffsrechten anmelden können, die sie zur Behebung von Problemen auf einem bestimmten System in diesem Netzwerk benötigen. Benutzerbasierte Richtlinien *können* auch systembasierte Kriterien enthalten.

- *Systembasierte Richtlinien* – Das sind Richtlinien, die nur systembasierte Kriterien enthalten. So können Sie zum Beispiel eine Richtlinienzuweisungsregel erstellen, die bei allen Servern im Netzwerk, die mit bestimmten Tags gekennzeichnet sind, oder auf allen Systemen, die sich in einem bestimmten Speicherort in der Systemstruktur befinden, umgesetzt wird. Systembasierte Richtlinien können *keine* benutzerbasierten Kriterien enthalten.

Priorität von Richtlinienzuweisungsregeln

Richtlinienzuweisungsregeln können priorisiert werden, um die Wartung der Richtlinienzuweisungsverwaltung zu vereinfachen. Wenn Sie für eine Regel eine Priorität festlegen, wird sie vor anderen Zuweisungen mit einer niedrigeren Priorität erzwungen.

In einigen Fällen kann dies dazu führen, dass Regeleinstellungen außer Kraft gesetzt werden. Beispiel: Ein Benutzer oder ein System ist in zwei Richtlinienzuweisungsregeln (Regel A und B) enthalten. Die Regel A hat die Prioritätsstufe 1 und räumt den zugehörigen Benutzern einen unbegrenzten Zugriff auf Internetinhalte ein. Die Regel B hat die Prioritätsstufe 2 und schränkt den Zugriff desselben Benutzers auf Internetinhalte stark ein. In diesem Szenario wird die Regel A erzwungen, da sie eine höhere Priorität hat. Daher hat der Benutzer uneingeschränkten Zugriff auf Internetinhalte.

Zusammenarbeit von Richtlinien für mehrere Richtlinienplätze mit der Priorität von Richtlinienzuweisungsregeln

Die Priorität von Regeln wird bei Richtlinien für mehrere Richtlinienplätze nicht berücksichtigt. Wenn eine einzelne Regel angewendet wird, die Richtlinien für mehrere Richtlinienplätze derselben Produktkategorie enthält, werden alle Einstellungen der Richtlinien für mehrere Richtlinienplätze kombiniert. Ebenso werden beim Anwenden mehrerer Regeln, die Einstellungen für Richtlinien für mehrere Richtlinienplätze enthalten, alle Einstellungen aus den einzelnen Richtlinien für mehrere Richtlinienplätze kombiniert. Dadurch besteht die angewendete Richtlinie aus einer Kombination der Einstellungen aller einzelnen Regeln.

Wenn Richtlinien für mehrere Richtlinienplätze aggregiert werden, erfolgt dies nur mit Richtlinien für mehrere Richtlinienplätze des gleichen Typs (benutzer- oder systemspezifisch). Richtlinien für mehrere Richtlinienplätze, die mittels Richtlinienzuweisungsregeln zugewiesen sind, werden jedoch nicht mit Richtlinien für mehrere Richtlinienplätze aggregiert, die in der Systemstruktur zugewiesen sind. In der Systemstruktur zugewiesene Richtlinien für mehrere Richtlinienplätze werden von Richtlinien für

mehrere Richtlinienplätze überschrieben, die mittels Richtlinienzuweisungsregeln zugewiesen sind. Außerdem haben benutzerbasierte Richtlinien Vorrang vor systembasierten Richtlinien. Betrachten wir das folgende Szenario, in dem Folgendes gilt:

Richtlinientyp	Zuweisungstyp	Richtlinienname	Richtlinieneinstellungen
Allgemeine Richtlinie	In der Systemstruktur zugewiesene Richtlinie	A	Unterbindet den Internetzugriff auf allen Systemen, denen die Richtlinie zugewiesen ist.
Systembasiert	Richtlinienzuweisungsregel	B	Erlaubt den Internetzugriff auf Systemen, die mit dem Tag "istLaptop" gekennzeichnet sind.
Benutzerbasiert	Richtlinienzuweisungsregel	C	Erlaubt allen Benutzern aus der Benutzergruppe "admin" auf allen Systemen den uneingeschränkten Internetzugriff.

Szenario: Steuerung des Internetzugriffs mithilfe von Richtlinien für mehrere Richtlinienplätze

In Ihrer Systemstruktur befindet sich eine Gruppe mit dem Namen "Technik", die aus Systemen besteht, die mit dem Tag "istServer" oder "istLaptop" gekennzeichnet sind. Richtlinie A ist in der Systemstruktur allen Systemen in dieser Gruppe zugewiesen. Wenn Richtlinie B mittels einer Richtlinienzuweisungsregel an einer beliebigen Stelle oberhalb der Gruppe "Technik" in der Systemstruktur zugewiesen wird, überschreibt sie die Einstellungen der Richtlinie A und erlaubt Systemen, die mit dem Tag "istLaptop" versehen sind, den Zugriff auf das Internet. Wenn Richtlinie C einer beliebigen Gruppe zugewiesen wird, die sich in der Systemstruktur oberhalb der Gruppe "Technik" befindet, wird dadurch Benutzern aus der Benutzergruppe "Admin" der Internetzugriff auf allen Systemen erlaubt, d. h. auch auf denjenigen, die sich in der Gruppe "Technik" befinden und mit "istServer" gekennzeichnet sind.

Ausschließen von Active Directory-Objekten aus aggregierten Richtlinien

Da Regeln, die aus Richtlinien für mehrere Richtlinienplätze bestehen, ohne Beachtung von Prioritäten auf zugewiesene Systeme angewendet werden, muss die Aggregation von Richtlinieneinstellungen an einigen Stellen möglicherweise verhindert werden. Die Aggregation von Einstellungen aus benutzerbasierten Richtlinien für mehrere Richtlinienplätze über mehrere Richtlinienzuweisungsregeln hinweg lässt sich verhindern, indem Sie einen Benutzer (oder andere Active Directory-Objekte wie eine Gruppe oder Organisationseinheit) beim Erstellen der Richtlinienzuweisungsregel ausschließen. Weitere Informationen zur Verwendung von Richtlinien für mehrere Richtlinienplätze in Richtlinienzuweisungsregeln finden Sie in der Produktdokumentation des von Ihnen verwendeten verwalteten Produkts.

Informationen zu benutzerbasierten Richtlinienzuweisungen

Mit benutzerbasierten Richtlinienzuweisungsregeln können Sie benutzerspezifische Richtlinienzuweisungen erstellen.

Diese Zuweisungen werden auf dem Zielsystem erzwungen, wenn sich ein Benutzer anmeldet.

Auf einem verwalteten System erfasst der Agent die Benutzer, die sich beim Netzwerk anmelden. Die Richtlinienzuweisungen, die Sie für die einzelnen Benutzer erstellen, werden auf das System gepusht, an dem sich diese Benutzer anmelden, und während jeder Agent-zu-Server-Kommunikation zwischengespeichert. Der Agent wendet die Richtlinien an, die Sie jedem Benutzer zugewiesen haben.



Wenn sich ein Benutzer zum ersten Mal an einem verwalteten System anmeldet, kann es zu einer geringfügigen Verzögerung kommen, während der Agent Kontakt zum zugewiesenen Server aufnimmt, um die für diesen Benutzer spezifischen Richtlinienzuweisungen abzurufen. Während dieses Zeitraums kann der Benutzer nur auf die Funktionen zugreifen, die von der Standardrichtlinie auf dem Computer – dies ist in der Regel die sicherste Richtlinie – zugelassen werden.



Wenn Sie benutzerbasierte Richtlinienzuweisungen verwenden möchten, müssen Sie einen LDAP-Server registrieren und für den Gebrauch bei Ihrem ePolicy Orchestrator-Server konfigurieren.

Informationen zum Migrieren älterer Richtlinienzuweisungsregeln

Richtlinienzuweisungsregeln, die mit einem ePolicy Orchestrator-Server der Version 4.5 erstellt wurden, sind standardmäßig benutzerbasiert. Migrierte ältere Richtlinienzuweisungsregeln, in denen keine benutzerdefinierten Kriterien angegeben sind, werden als benutzerbasiert ausgewertet. Wenn Sie jedoch eine neue benutzerbasierte Richtlinienzuweisungsregel erstellen, müssen Sie mindestens ein benutzerbasiertes Kriterium angeben.



Wenn migrierte ältere benutzerbasierte Richtlinienzuweisungsregeln angewendet werden, schlägt der ePolicy Orchestrator-Server jedes verwaltete System im Netzwerk in jedem Agent-zu-Server-Kommunikationsintervall auf dem LDAP-Server nach.

Informationen zu systembasierten Richtlinienzuweisungen

Mithilfe systembasierter Richtlinien können Systemen Richtlinien nach systembasierten Kriterien zugewiesen werden.

Eine systembasierte Richtlinie kann mithilfe zweier Typen von systembasierten Kriterien zugewiesen werden:

- **Speicherort in der Systemstruktur** – Bei allen Richtlinienzuweisungsregeln muss ein Speicherort in der Systemstruktur angegeben werden.
- **Tags** – Richtlinien müssen Systemen anhand der angewendeten Tags zugewiesen werden.

Sobald Sie ein Tag definiert und auf Systeme angewendet haben, können Sie eine Richtlinienzuweisungsregel erstellen, nach der Richtlinien auf jedes System angewendet werden sollen, das mit diesem Tag gekennzeichnet ist. Diese Funktion ist besonders nützlich, wenn alle Systeme eines bestimmten Typs über die gleiche Sicherheitsrichtlinie verfügen sollen, unabhängig von ihrer Position in der Systemstruktur.

Zuweisen von systembasierten Richtlinien mithilfe von Tags

Mithilfe von Tags zum Zuweisen systembasierter Richtlinien wird die Automatisierung der Richtlinienzuweisung vereinfacht.

Systembasierte Richtlinien, in denen als Kriterien Tags angegeben sind, arbeiten ähnlich wie benutzerbasierte Richtlinien. Ihre Zuweisung erfolgt anhand von Auswahlkriterien, die Sie im **Generator für Richtlinienzuweisungen** definieren. Sie können jedem System, das mit einem Tag versehen werden kann, anhand dieses Tags eine bestimmte Richtlinie zuweisen.

Szenario: Erstellen neuer SuperAgents mithilfe von Tags

Sie möchten einen neuen Satz von SuperAgents in Ihrer Umgebung erstellen, haben jedoch nicht die Zeit, manuell die Systeme in der **Systemstruktur** zu bestimmen, auf denen sich diese SuperAgents befinden sollen. Stattdessen können Sie den **Tag-Generator** verwenden, um alle Systeme, die den

gewünschten Kriterien entsprechen, mit einem neuen Tag zu kennzeichnen: "istSuperAgent". Nachdem Sie das Tags erstellt haben, können Sie eine Richtlinienzuweisungsregel erstellen, die Ihre SuperAgent-Richtlinieneinstellungen auf alle Systeme anwendet, die mit dem Tag "istSuperAgent" gekennzeichnet sind.

Sobald Sie das Tag erstellt haben, können Sie die Aktion **Tag-Kriterien ausführen** auf der Seite **Tag-Katalog** verwenden, damit jedem mit dem neuen Tag versehenen System, wenn es sich in regelmäßigen Abständen meldet, die neue Richtlinie gemäß Ihrer Richtlinienzuweisungsregel "istSuperAgent" zugewiesen wird.

Erstellen von Richtlinienzuweisungsregeln

Durch die Erstellung von Richtlinienzuweisungsregeln können Sie Richtlinien für Benutzer oder Systeme anhand konfigurierter Regelkriterien erzwingen.

Vorgehensweise

Definitionen zu Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

1. Klicken Sie auf **Menü** | **Richtlinie** | **Richtlinienzuweisungsregeln**, und klicken Sie dann auf **Aktionen** | **Neue Zuweisungsregel**. Der **Generator für Richtlinienzuweisungen** wird mit der Seite **Details** geöffnet.
2. Geben Sie die Details für diese Richtlinienzuweisungsregel an. Dazu gehören die folgenden:
   - Ein eindeutiger **Name** und eine **Beschreibung**.
   - Der **Regeltyp**. Von dem von Ihnen angegebenen Regeltyp hängt es ab, welche Kriterien im Schritt **Auswahlkriterien** verfügbar sind.

   
   Die Priorität für neue Richtlinienzuweisungsregeln wird standardmäßig sequenziell basierend auf der Anzahl vorhandener Regeln zugewiesen. Nachdem Sie die Regel erstellt haben, können Sie die Priorität bearbeiten, indem Sie auf der Seite **Richtlinienzuweisungsregeln** auf **Priorität bearbeiten** klicken.
3. Klicken Sie auf **Weiter**. Die Seite **Zugewiesene Richtlinien** wird geöffnet.
4. Klicken Sie auf **Richtlinie hinzufügen**, um die Richtlinien auszuwählen, die von dieser Richtlinienzuweisungsregel erzwungen werden sollen.
5. Klicken Sie auf **Weiter**. Die Seite **Auswahlkriterien** wird geöffnet.
6. Geben Sie die Kriterien an, die in dieser Regel verwendet werden sollen. Ihre Kriterienauswahl bestimmt, welchen Systemen oder Benutzern diese Richtlinie zugewiesen wird.
7. Überprüfen Sie die Zusammenfassung, und klicken Sie dann auf **Speichern**.

Verwalten von Richtlinienzuweisungsregeln

Verwenden Sie die in dieser Aufgabe gezeigte Tabelle, um bei der Arbeit mit Richtlinienzuweisungsregeln allgemeine Verwaltungs-Tasks durchzuführen.

Klicken Sie zum Durchführen dieser Aktionen auf **Menü** | **Richtlinie** | **Richtlinienzuweisungsregeln**. Wählen Sie die Aktion, die Sie ausführen möchten, im Menü **Aktionen** oder in der Spalte **Aktionen** aus.

Aktion	Vorgehensweise
Löschen von Richtlinienzuweisungsregeln	Klicken Sie in der Zeile mit der ausgewählten Zuweisung auf **Löschen**.
Bearbeiten von Richtlinienzuweisungsregeln	Klicken Sie auf die ausgewählte Zuweisung. Der Assistent **Generator für Richtlinienzuweisungen** wird angezeigt. Führen Sie die Schritte auf den einzelnen Seiten des Assistenten durch, um diese Richtlinienzuweisungsregel zu ändern.

Aktion	Vorgehensweise
Exportieren von Richtlinienzuweisungsregeln	Klicken Sie auf **Exportieren**. Die Seite **Exportieren** wird geöffnet, auf der Sie die Datei POLICYASSIGNMENTRULES.XML anzeigen oder herunterladen können.
Importieren von Richtlinienzuweisungsregeln	Klicken Sie auf **Importieren**. Das Dialogfeld **Aktion: Importieren** wird geöffnet, in dem Sie die zuvor heruntergeladene Datei POLICYASSIGNMENTRULES.XML suchen können. Sie werden aufgefordert, die in der Datei enthaltenen Regeln auszuwählen, die importiert werden sollen. Sie können auswählen, welche Regeln importiert werden sollen. Falls Regeln in der Datei einen identischen Namen haben wie Regeln, die sich bereits in der Liste **Richtlinienzuweisungsregeln** befinden, können Sie darüber hinaus auswählen, welche Regeln beibehalten werden sollen.
Bearbeiten der Priorität einer Richtlinienzuweisungsregel	Klicken Sie auf **Priorität bearbeiten**. Die Seite **Richtlinienzuweisungsregeln | Priorität bearbeiten** wird geöffnet, auf der Sie die Priorität von Richtlinienzuweisungsregeln mittels Ziehen und Ablegen ändern.
Anzeigen der Zusammenfassung einer Richtlinienzuweisungsregel	Klicken Sie in der Zeile mit der ausgewählten Zuweisung auf **>**.

Erstellen von Abfragen zur Richtlinienverwaltung

Sie können die einem verwalteten System zugewiesenen oder die in der Systemhierarchie unterbrochenen Richtlinien abrufen.

Dazu können Sie eine der folgenden Abfragen zur Richtlinienverwaltung erstellen:

- **Angewendete Richtlinien** – Diese Abfrage ruft Richtlinien ab, die einem angegebenen verwalteten System zugewiesen sind.
- **Vererbung unterbrochen** – Diese Abfrage ruft Informationen zu Richtlinien ab, die in der Systemhierarchie unterbrochen sind.

Vorgehensweise

Definitionen zu Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

1. Klicken Sie auf **Menü** | **Berichterstellung** | **Abfragen und Berichte**, und klicken Sie dann auf **Aktionen** | **Neu**.

   Der **Abfragen-Generator** wird geöffnet.
2. Wählen Sie auf der Seite **Ergebnistyp** in der Liste **Funktionsgruppe** den Eintrag **Richtlinienverwaltung** aus.
3. Wählen Sie einen der angezeigten Ergebnistypen aus, und klicken Sie dann auf **Weiter**, um die Seite **Diagramm** zu öffnen.
   - **Angewandte Client-Tasks**
   - **Angewendete Richtlinien**
   - **Unterbrochene Vererbung für Client-Task-Zuweisung**
   - **Unterbrochene Vererbung für Richtlinienzuweisung**
4. Wählen Sie den Typ von Diagramm oder Tabelle aus, mit dem die primären Ergebnisse der Abfrage dargestellt werden sollen, und klicken Sie dann auf **Weiter**.

   Die Seite **Spalten** wird angezeigt.

   Wenn Sie **Boolesches Kreisdiagramm** auswählen, müssen Sie die Kriterien konfigurieren, die in der Abfrage enthalten sein sollen.

5 Wählen Sie die Spalten aus, die in der Abfrage enthalten sein sollen, und klicken Sie dann auf **Weiter**.

  Die Seite **Filter** wird angezeigt.

6 Wählen Sie Eigenschaften aus, um die Suchergebnisse einzugrenzen, und klicken Sie dann auf **Ausführen**.

  Auf der Seite **Ungespeicherte Abfrage** werden die Ergebnisse der Abfrage angezeigt, an denen auch Aktionen durchgeführt werden können.

  Ausgewählte Eigenschaften werden im Inhaltsbereich mit Operatoren angezeigt, die Kriterien festlegen können, nach denen die für die jeweilige Eigenschaft zurückgegebenen Daten eingegrenzt werden.

7 Auf der Seite **Ungespeicherte Abfrage** können Sie an Elementen, die in Tabellen oder Aufgliederungstabellen aufgeführt sind, alle zur Verfügung stehenden Aktionen durchführen.

- Wenn die Abfrage nicht die erwarteten Ergebnisse zurückgegeben hat, klicken Sie auf **Abfrage bearbeiten**, um zum **Abfragen-Generator** zurückzukehren und die Details der Abfrage zu bearbeiten.
- Wenn Sie die Abfrage nicht speichern möchten, klicken Sie auf **Schließen**.
- Wenn Sie diese Abfrage zu einem späteren Zeitpunkt erneut verwenden möchten, klicken Sie auf **Speichern**, und fahren Sie dann mit dem nächsten Schritt fort.

8 Geben Sie auf der Seite **Abfrage speichern** einen Namen für die Abfrage ein, fügen Sie Anmerkungen hinzu, und wählen Sie dann eine der folgenden Optionen aus:

- **Neue Gruppe** – Geben Sie den Namen der neuen Gruppe ein, und wählen Sie eine der folgenden Optionen:
  - **Private Gruppe (Eigene Gruppen)**
  - **Öffentliche Gruppe (Freigegebene Gruppen)**
- **Vorhandene Gruppe** – Wählen Sie die Gruppe in der Liste **Freigegebene Gruppen** aus.

9 Klicken Sie auf **Speichern**.

Anzeigen der Richtlinieninformationen

Sie können detaillierte Informationen zu Richtlinien anzeigen, darunter Informationen über die Besitzer, die Zuweisungen und die Vererbung.

Aufgaben

- *Anzeigen der Gruppen und Systeme, denen eine Richtlinie zugewiesen ist* auf Seite 199

  Sie können Gruppen und Systeme anzeigen, denen eine Richtlinie zugewiesen ist. In dieser Liste werden nur die Zuweisungspunkte angezeigt, aber nicht die einzelnen Knoten oder Systeme, die diese Richtlinie erben.
- *Anzeigen von Richtlinieneinstellungen* auf Seite 199

  Sie können Details zu einer Richtlinie anzeigen, die einer Produktkategorie oder einem System zugewiesen ist.
- *Anzeigen des Richtlinienbesitzes* auf Seite 200

  Sie können die Besitzer einer Richtlinie anzeigen.
- *Anzeigen von Zuweisungen, bei denen die Richtlinienerzwingung deaktiviert ist* auf Seite 200

  Sie können Zuweisungen anzeigen, bei denen die Richtlinienerzwingung (pro Richtlinienkategorie) deaktiviert ist.
- *Anzeigen der einer Gruppe zugewiesenen Richtlinien* auf Seite 200

  Sie können die einer Systemstrukturgruppe zugewiesenen Richtlinien nach Produkt sortiert anzeigen.
- *Anzeigen der einem bestimmten System zugewiesenen Richtlinien* auf Seite 201

  Sie können die Richtlinien anzeigen, die einem bestimmten System in der Systemstrukturgruppe zugewiesen worden.
- *Anzeigen der Richtlinienvererbung für eine Gruppe* auf Seite 201

  Sie können die Richtlinienvererbung einer bestimmten Gruppe anzeigen.
- *Anzeigen und Zurücksetzen einer unterbrochenen Vererbung* auf Seite 201

  Sie können die Gruppen und Systeme ermitteln, bei denen die Richtlinienvererbung unterbrochen wurde.
- *Vergleichen von Richtlinien* auf Seite 202

  Mithilfe der Option **Richtlinienvergleich** können Sie Richtlinien vergleichen. Auf diese Weise können Sie feststellen, welche Einstellungen identisch und welche unterschiedlich sind.

Anzeigen der Gruppen und Systeme, denen eine Richtlinie zugewiesen ist

Sie können Gruppen und Systeme anzeigen, denen eine Richtlinie zugewiesen ist. In dieser Liste werden nur die Zuweisungspunkte angezeigt, aber nicht die einzelnen Knoten oder Systeme, die diese Richtlinie erben.

Vorgehensweise

Definitionen zu Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

1. Klicken Sie auf **Menü** | **Richtlinie** | **Richtlinienkatalog**, und wählen Sie dann das gewünschte **Produkt** und die gewünschte **Kategorie** aus.

   Alle für die ausgewählte Kategorie erstellten Richtlinien werden im Detailbereich angezeigt.
2. Klicken Sie unter **Zuweisungen** in der Zeile der gewünschten Richtlinie auf den Link, der die Anzahl der Gruppen oder Systeme angibt, denen die Richtlinie zugewiesen ist (z. B. **6 Zuweisungen**).

   Auf der Seite **Zuweisungen** werden alle Gruppe oder Systeme, denen die Richtlinie zugewiesen ist, mit ihrem **Knotennamen** und **Knotentyp** angezeigt.

Anzeigen von Richtlinieneinstellungen

Sie können Details zu einer Richtlinie anzeigen, die einer Produktkategorie oder einem System zugewiesen ist.

Vorgehensweise

Definitionen zu Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

1. Klicken Sie auf **Menü | Richtlinie | Richtlinienkatalog**, und wählen Sie dann das gewünschte **Produkt** und die gewünschte **Kategorie** aus.

   Alle für die ausgewählte Kategorie erstellten Richtlinien werden im Detailbereich angezeigt.

2. Klicken Sie neben die gewünschte Richtlinie.

   Die Richtlinienseiten werden mit den Einstellungen der Richtlinie angezeigt.

   Sie können diese Informationen auch anzeigen, wenn Sie auf die einer bestimmten Gruppe zugewiesenen Richtlinien zugreifen. Klicken Sie zum Zugriff auf diese Informationen auf **Menü | Systeme | Systemstruktur | Zugewiesene Richtlinien** und anschließend in der Spalte **Richtlinie** auf den Link für die ausgewählte Richtlinie.

Anzeigen des Richtlinienbesitzes

Sie können die Besitzer einer Richtlinie anzeigen.

Vorgehensweise

Definitionen zu Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

1. Klicken Sie auf **Menü | Richtlinie | Richtlinienkatalog**, und wählen Sie dann das gewünschte **Produkt** und die gewünschte **Kategorie** aus.

   Alle für die ausgewählte Kategorie erstellten Richtlinien werden im Detailbereich angezeigt.

2. Die Besitzer der Richtlinie werden unter **Besitzer** angezeigt.

Anzeigen von Zuweisungen, bei denen die Richtlinienerzwingung deaktiviert ist

Sie können Zuweisungen anzeigen, bei denen die Richtlinienerzwingung (pro Richtlinienkategorie) deaktiviert ist.

Vorgehensweise

Definitionen zu Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

1. Klicken Sie auf **Menü | Richtlinie | Richtlinienkatalog**, und wählen Sie dann das gewünschte **Produkt** und die gewünschte **Kategorie** aus.

   Alle für die ausgewählte Kategorie erstellten Richtlinien werden im Detailbereich angezeigt.

2. Klicken Sie auf den Link neben **Erzwingungsstatus für Produkt**, der die Anzahl der Zuweisungen anzeigt, bei denen die Erzwingung deaktiviert ist (sofern vorhanden).

   Die Seite **Erzwingen für <Richtlinienname>** wird angezeigt.

3. Klicken Sie auf ein beliebiges Element in der Liste, um zu dessen Seite **Zugewiesene Richtlinien** zu wechseln.

Anzeigen der einer Gruppe zugewiesenen Richtlinien

Sie können die einer Systemstrukturgruppe zugewiesenen Richtlinien nach Produkt sortiert anzeigen.

Vorgehensweise

Definitionen zu Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

1. Klicken Sie auf **Menü | Systeme | Systemstruktur | Zugewiesene Richtlinien**, und wählen Sie dann in der Systemstruktur eine Gruppe aus.

   Im Detailbereich werden alle zugewiesenen Richtlinien nach Produkt geordnet angezeigt.

2. Klicken Sie auf eine beliebige Richtlinie, um deren Einstellungen anzuzeigen.

Anzeigen der einem bestimmten System zugewiesenen Richtlinien

Sie können die Richtlinien anzeigen, die einem bestimmten System in der Systemstrukturgruppe zugewiesen worden.

Vorgehensweise

Definitionen zu Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

1. Klicken Sie auf **Menü | Systeme | Systemstruktur | Systeme**, und wählen Sie dann in der Systemstruktur die gewünschte Gruppe aus.

   Alle Systeme, die zu der Gruppe gehören, werden im Detailbereich angezeigt.

2. Wählen Sie das System aus, und klicken Sie auf **Aktionen | Agent | Richtlinien auf einem einzelnen System ändern**.

3. Wählen Sie das Produkt aus.

   Die diesem System für das Produkt zugewiesenen Richtlinien werden angezeigt.

4. Klicken Sie auf eine beliebige Richtlinie, um deren Einstellungen anzuzeigen.

Anzeigen der Richtlinienvererbung für eine Gruppe

Sie können die Richtlinienvererbung einer bestimmten Gruppe anzeigen.

Definitionen zu Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

Vorgehensweise

1. Klicken Sie auf **Menü | Systeme | Systemstruktur | Zugewiesene Richtlinien**.

   Im Detailbereich werden alle zugewiesenen Richtlinien nach Produkt geordnet angezeigt.

2. In der gewünschten Richtlinienzeile unter **Erben von** ist der Name der Gruppe aufgeführt, von der die Richtlinie vererbt wurde.

Anzeigen und Zurücksetzen einer unterbrochenen Vererbung

Sie können die Gruppen und Systeme ermitteln, bei denen die Richtlinienvererbung unterbrochen wurde.

Vorgehensweise

Definitionen zu Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

1. Klicken Sie auf **Menü** | **Systeme** | **Systemstruktur** | **Zugewiesene Richtlinien**.

   Im Detailbereich werden alle zugewiesenen Richtlinien nach Produkt geordnet angezeigt. In der Zeile mit der gewünschten Richtlinie ist unter **Vererbung unterbrochen** die Anzahl der Gruppen und Systeme aufgeführt, bei denen die Vererbung dieser Richtlinie unterbrochen ist.

   Dies ist die Anzahl der Gruppen bzw. Systeme, bei denen die Richtlinienvererbung unterbrochen ist, nicht die Anzahl der Systeme, die die Richtlinie nicht erben. Wenn beispielsweise nur eine Gruppe die Richtlinie nicht erbt, wird dies durch **1 erbt nicht** angezeigt, unabhängig von der Anzahl der Systeme innerhalb der Gruppe.

2. Klicken Sie auf den Link, der die Anzahl der untergeordneten Gruppen oder Systeme anzeigt, bei denen die Vererbung unterbrochen ist.

   Die Seite **Unterbrochene Vererbung: Anzeigen** wird mit einer Liste der Namen dieser Gruppen und Systeme angezeigt.

3. Aktivieren Sie zum Zurücksetzen der Vererbung einer dieser Gruppen oder eines dieser Systeme das Kontrollkästchen neben dem Namen, klicken Sie dann auf **Aktionen**, und wählen Sie **Vererbung zurücksetzen** aus.

Vergleichen von Richtlinien

Mithilfe der Option **Richtlinienvergleich** können Sie Richtlinien vergleichen. Auf diese Weise können Sie feststellen, welche Einstellungen identisch und welche unterschiedlich sind.

Viele der im Richtlinienvergleich enthaltenen Werte und Variablen sind produktspezifisch. Informationen zu Optionen, die nicht in der Tabelle aufgeführt sind, finden Sie in der Produktdokumentation des jeweiligen Produkts, von dem die Richtlinie stammt, die Sie vergleichen möchten.

Vorgehensweise

Definitionen zu Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

1. Klicken Sie auf **Menü** | **Richtlinienvergleich**, und wählen Sie dann in den Listen die gewünschten Einstellungen für **Produkt**, **Kategorie** und **Anzeigen** aus.

   Mit diesen Einstellungen werden die zu vergleichenden Richtlinien in den Listen **Richtlinie 1** und **Richtlinie 2** aufgefüllt.

2. Wählen Sie die zu vergleichenden Richtlinien in der Zeile **Richtlinien vergleichen** in den Spalten der Listen **Richtlinie 1** und **Richtlinie 2** aus.

   In den beiden obersten Zeilen der Tabelle wird angezeigt, wie viele Einstellungen unterschiedlich und wie viele identisch sind. Wenn weniger Daten angezeigt werden sollen, können Sie auch die Einstellung **Anzeigen** von **Alle Richtlinieneinstellungen** in **Unterschiede zwischen Richtlinien** oder **Übereinstimmungen zwischen Richtlinien** ändern.

3. Klicken Sie auf **Drucken**, um eine druckfähige Ansicht des Vergleichs anzuzeigen.

Freigeben von Richtlinien zwischen McAfee ePO-Servern

Durch Freigeben von Richtlinien können Administratoren Richtlinien bestimmen, die auf einem Server entwickelt wurden und auf den anderen Servern implementiert werden sollen.

Dazu müssen Administratoren nur drei Schritte durchführen.

1. Bestimmen der freizugebenden Richtlinie
2. Registrieren der Server, die die Richtlinie gemeinsam verwenden sollen
3. Planen eines Server-Tasks zum Verteilen der freigegebenen Richtlinie

Verteilen einer Richtlinie an mehrere McAfee ePO-Server

Sie können die Richtlinienfreigabe zur Verwendung mit mehreren McAfee ePO-Servern konfigurieren. Es wird empfohlen, diese Aufgaben in der hier aufgeführten Reihenfolge auszuführen.



Wenn die Richtlinie nach der Freigabe geändert werden muss, bearbeiten Sie die Richtlinie, und führen Sie den Task zur Richtlinienfreigabe erneut aus. Sie sollten die lokalen Administratoren über die Änderung informieren.

Aufgaben

- *Registrieren von Servern zur Richtlinienfreigabe* auf Seite 203
  Sie können Server registrieren, sodass sie Richtlinien freigeben.
- *Bestimmen von Richtlinien zur Freigabe* auf Seite 203
  Sie können festlegen, dass eine Richtlinie für mehrere McAfee ePO-Server freigegeben werden soll.
- *Planen von Server-Tasks zum Freigeben von Richtlinien* auf Seite 204
  Sie können einen Server-Task planen, damit Richtlinien für mehrere McAfee ePO-Server freigegeben werden.

Registrieren von Servern zur Richtlinienfreigabe

Sie können Server registrieren, sodass sie Richtlinien freigeben.

Definitionen zu Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

Vorgehensweise

1. Klicken Sie auf **Menü** | **Konfiguration** | **Registrierte Server**, und klicken Sie dann auf **Neuer Server**. Der Assistent **Generator für registrierte Server** wird mit der Seite **Beschreibung** geöffnet.
2. Wählen Sie im Menü **Server-Typ** den Eintrag **ePO** aus, geben Sie einen Namen und eventuelle Anmerkungen ein, und klicken Sie dann auf **Weiter**. Die Seite **Details** wird angezeigt.
3. Geben Sie die Details zu Ihrem Server an, klicken Sie für **Richtlinienfreigabe** auf **Aktivieren**, und klicken Sie dann auf **Speichern**.

Bestimmen von Richtlinien zur Freigabe

Sie können festlegen, dass eine Richtlinie für mehrere McAfee ePO-Server freigegeben werden soll.

Vorgehensweise

Definitionen zu Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

1. Klicken Sie auf **Menü** | **Richtlinie** | **Richtlinienkatalog**, klicken Sie dann auf das Dropdown-Menü **Produkt**, und wählen Sie das Produkt aus, dessen Richtlinie Sie freigeben möchten.
2. Klicken Sie in der Spalte **Aktionen** für die freizugebende Richtlinie auf **Freigeben**.

Ab ePolicy Orchestrator 4.6 werden freigegebene Richtlinien automatisch zu ePolicy Orchestrator-Servern gepusht, bei denen die Richtlinienfreigabe aktiviert ist. Wenn Sie in Schritt 2 auf **Freigeben** klicken, wird die Richtlinie unverzüglich zu allen registrierten ePolicy Orchestrator-Servern gepusht, bei denen die Richtlinienfreigabe aktiviert ist. Auf ähnliche Weise werden auch Änderungen an freigegebenen Richtlinien gepusht.

Planen von Server-Tasks zum Freigeben von Richtlinien

Sie können einen Server-Task planen, damit Richtlinien für mehrere McAfee ePO-Server freigegeben werden.

Vorgehensweise

Definitionen zu Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

1. Klicken Sie auf **Menü** | **Automatisierung** | **Server-Tasks**, und klicken Sie dann auf **Aktionen** | **Neuer Task**. Der Assistent **Generator für Server-Tasks** wird geöffnet.
2. Geben Sie auf der Seite **Beschreibung** den Namen des Tasks und eventuelle Anmerkungen ein, und klicken Sie dann auf **Weiter**. Die Seite **Aktionen** wird angezeigt.



Neue Server-Tasks sind standardmäßig aktiviert. Wenn dieser Task nicht aktiviert sein soll, wählen Sie im Feld **Planungsstatus** die Option **Deaktiviert** aus.

3. Wählen Sie im Dropdown-Menü **Aktionen** den Eintrag **Richtlinien freigeben** aus, und klicken Sie dann auf **Weiter**. Die Seite **Plan** wird angezeigt.
4. Geben Sie den Zeitplan für den Task an, und klicken Sie dann auf **Weiter**. Die Seite **Zusammenfassung** wird geöffnet.
5. Überprüfen Sie die zusammengefassten Informationen, und klicken Sie dann auf **Speichern**.

14 Client- und Server-Tasks

Mithilfe von Client- und Server-Tasks können Sie die Verwaltung der auf den Systemen in einem Netzwerk ausgebrachten Sicherheits-Software automatisieren.

Das Verwalten von Produkten von einer zentralen Stelle aus ist eine Hauptfunktion von ePolicy Orchestrator. Erreichen können Sie dies u. a., indem Sie Client- und Server-Tasks erstellen und planen. Bei beiden handelt es sich um geplante Aktionen, die auf dem Server oder auf verwalteten Systemen ausgeführt werden, um sicherzustellen, dass in einem Netzwerk die aktuellsten Sicherheitsinhalte ausgebracht sind.

Inhalt

Erstmaliges Konfigurieren von Tasks

Gehen Sie wie nachfolgend allgemein beschrieben vor, wenn Sie zum ersten Mal Client- und Server-Tasks konfigurieren.

1. Planen Sie Client-Tasks für die Segmente Ihrer Systemstruktur.
2. Erstellen Sie Client-Tasks für Gruppen und Systeme, und weisen Sie sie zu.
3. Erstellen Sie Server-Tasks, um Ihre Repositories auf dem aktuellen Stand zu halten und Server-Wartungsarbeiten zu automatisieren.
4. Planen Sie Tasks zur automatischen Ausführung.

Client-Tasks

Sie können Client-Tasks erstellen und planen, um die Verwaltung der Systeme in Ihrem Netzwerk zu automatisieren.

Welche Client-Tasks verfügbar sind, richtet sich nach den auf dem McAfee ePO-Server installierten Erweiterungsdateien.

Client-Tasks werden für gewöhnlich für folgende Zwecke verwendet:

- Produktausbringung
- Produktfunktionalität (z. B. der Task "On-Demand-Scan" von VirusScan Enterprise)
- Upgrades und Aktualisierungen

Weitere Informationen dazu, welche Client-Tasks verfügbar sind und bei welchen Arbeiten diese Tasks Sie unterstützen, finden Sie in der Produktdokumentation Ihrer verwalteten Produkte.

Funktionsweise des Client-Task-Katalogs

Im Client-Task-Katalog können Sie Client-Task-Objekte erstellen, die Sie auch zur Verwaltung der Systeme in einem Netzwerk verwenden können.

Der Client-Task-Katalog wendet das Konzept logischer Objekte auf ePolicy Orchestrator-Client-Tasks an. Sie können Client-Task-Objekte für vielfältige Verwendungszwecke erstellen, ohne sie sofort zuweisen zu müssen. Daher können Sie diese Objekte beim Zuweisen und Planen von Client-Tasks als wiederverwendbare Komponenten betrachten.

Client-Tasks können auf jeder beliebigen Ebene in der Systemstruktur zugewiesen werden und werden von den Gruppen und Systemen geerbt, die sich auf einer niedrigeren Ebene befinden. Wie bei Richtlinien und Richtlinienzuweisungen können Sie die Vererbung für einen zugewiesenen Client-Task unterbrechen.

Client-Task-Objekte können für mehrere registrierte ePolicy Orchestrator-Server in einer Umgebung freigegeben werden. Wenn Client-Task-Objekte als freigegeben festgelegt werden, erhält jeder registrierte Server nach Ausführung des Server-Tasks **Client-Task freigeben** eine Kopie. Alle am Task vorgenommenen Änderungen werden bei jedem Ausführen des Tasks aktualisiert. Wenn ein Client-Task-Objekt freigegeben ist, kann nur dessen Besitzer seine Einstellungen ändern.



Administratoren auf dem Ziel-Server, der einen freigegebenen Task empfängt, sind keine Besitzer dieses freigegebenen Tasks. Auch keiner der Benutzer auf dem Ziel-Server ist Besitzer von dort eingehenden freigegebenen Task-Objekten.

Ausbringungs-Tasks

Ausbringungs-Tasks sind Client-Tasks, mit denen verwaltete Sicherheitsprodukte aus dem Master-Repository auf verwalteten (Client-)Systemen ausgebracht werden.

Sie können einzelne Ausbringungs-Task-Objekte mithilfe des Client-Task-Katalogs erstellen sowie verwalten und sie dann Gruppen oder bestimmten Systemen zur Ausführung zuweisen. Alternativ dazu können Sie ab der Version 5.0 von ePolicy Orchestrator auch Produktausbringungsprojekte erstellen, um Produkte auf Systemen auszubringen. Produktausbringungsprojekte automatisieren die Erstellung und Planung einzelner Client-Task-Objekte. Darüber hinaus verfügen sie über zusätzliche automatisierte Verwaltungsfunktionen. Weitere Informationen über das Erstellen von Produktausbringungsprojekten finden Sie unter *Produktausbringung*.

Wenn Sie sich für eine Vorgehensweise für die Produktausbringung entscheiden, sollten Sie die Paketgröße und die verfügbare Netzwerkbandbreite zwischen den Master- oder verteilten Repositories und den verwalteten Systemen berücksichtigen. Zusätzlich zu einer eventuellen Überlastung des McAfee ePO-Servers oder Ihres Netzwerks kann bei einer Ausbringung auf zu vielen Systemen die Problembehandlung sehr kompliziert werden.

Möglicherweise ist es sinnvoll, die Produkte nacheinander auf Systemgruppen zu installieren. Wenn Ihre Netzwerkverbindungen schnell sind, versuchen Sie, die Ausbringung jeweils auf mehreren hundert Clients gleichzeitig durchzuführen. Bei langsameren oder weniger zuverlässigen Netzwerkverbindungen sollten Sie es mit kleineren Gruppen versuchen. Während der Ausbringung in der jeweiligen Gruppe sollten Sie die Ausbringung überwachen, Berichte zum Bestätigen erfolgreicher Installationen ausführen und Probleme mit einzelnen Systemen beheben.

Wenn Sie McAfee-Produkte oder -Komponenten ausbringen, die auf einem Teil Ihrer verwalteten Systeme installiert sind, gehen Sie wie folgt vor:

1. Verwenden Sie ein Tag, um diese Systeme zu identifizieren.
2. Verschieben Sie die gekennzeichneten Systeme in eine Gruppe.
3. Konfigurieren Sie einen Client-Task für die Produktausbringung für die Gruppe.

Ausbringungspakete für Produkte und Aktualisierungen

Die ePolicy Orchestrator-Ausbringungsinfrastruktur unterstützt sowohl das Ausbringen als auch das Aktualisieren von Produkten und Komponenten.

Jedes McAfee-Produkt, das von ePolicy Orchestrator ausgebracht werden kann, verfügt über eine Ausbringungspaketdatei im ZIP-Format. In dieser ZIP-Datei befinden sich Installationsdateien für das Produkt, die in einem sicheren Format komprimiert sind. Sobald diese Pakete in das Master-Repository eingecheckt sind, kann ePolicy Orchestrator sie auf jedem Ihrer verwalteten Systeme ausbringen.

Diese ZIP-Dateien werden sowohl für Virusdefinitionsdateien (DAT-Dateien) als auch für Scan-Modul-Aktualisierungspakete verwendet.

Die Produktrichtlinien können vor und nach der Ausbringung konfiguriert werden. Sie sollten die Richtlinieneinstellungen jedoch vor dem Ausbringen des Produkts in Ihren Netzwerksystemen konfigurieren. Damit sparen Sie Zeit und stellen sicher, dass Ihre Systeme zum frühestmöglichen Zeitpunkt geschützt werden.

Folgende Pakettypen können mithilfe von Abruf-Tasks oder manuell in das Master-Repository eingecheckt werden.

Unterstützte Pakettypen

Pakettyp	Beschreibung	Ursprung
SuperDAT-Dateien (SDAT.EXE) Dateityp: SDAT.EXE	Die SuperDAT-Dateien enthalten sowohl DAT- als auch Scan-Modul-Dateien in einem Aktualisierungspaket. Bei Problemen mit der Bandbreite sollten Sie DAT- und Scan-Modul-Dateien getrennt aktualisieren.	McAfee-Website. Laden Sie die SuperDAT-Dateien herunter, und checken Sie sie manuell in das Master-Repository ein.
Ergänzende Virusdefinitionsdateien (EXTRA.DAT) Dateityp: Extra.DAT	Die Extra.DAT-Dateien beziehen sich auf eine oder mehrere bestimmte Bedrohungen, die erst nach der zuletzt veröffentlichten DAT-Datei aufgetreten sind. Wenn eine ernsthafte Bedrohung vorliegt, sollten Sie die Extra.DAT-Datei sofort verteilen und nicht warten, bis die Signatur zur nächsten DAT-Datei hinzugefügt wird. Extra.DAT-Dateien werden auf der McAfee-Website veröffentlicht. Sie können sie mithilfe von ePolicy Orchestrator verteilen. Extra.DAT-Dateien werden nicht mit Abruf-Tasks abgerufen.	McAfee-Website. Laden Sie die zusätzlichen DAT-Dateien herunter, und checken Sie sie manuell in das Master-Repository ein.

Pakettyp	Beschreibung	Ursprung
Produktausbringungs- und Aktualisierungspakete Dateityp: ZIP	Produktausbringungspakete enthalten die Installationsdateien für ein McAfee-Produkt.	Produkt-CD oder heruntergeladene ZIP-Datei. Checken Sie Produktausbringungspakete manuell in das Master-Repository ein. In der Dokumentation für das jeweilige Produkt finden Sie die genauen Speicherorte.
Agenten-Sprachpakete Dateityp: ZIP	Agenten-Sprachpakete enthalten die Dateien, die für das Anzeigen der Agenten-Informationen in einer bestimmten Sprache erforderlich sind.	Master-Repository. Während der Installation eingecheckt. Bei zukünftigen Agenten-Versionen müssen die Agenten-Sprachpakete manuell in das Master-Repository eingecheckt werden.

Paket-Signaturen und Sicherheit

Alle von McAfee erstellten und verteilten Pakete werden mit einem Schlüsselpaar signiert, wobei das DSA-Signaturverifizierungssystem (Digital Signature Algorithm) und die 168-Bit-3DES-Verschlüsselung zum Einsatz kommen. Schlüssel werden verwendet, um vertrauliche Daten zu ver- oder entschlüsseln.

Sie werden benachrichtigt, wenn Sie Pakete einchecken, die nicht von McAfee signiert sind. Wenn Sie den Paketinhalt als gültig und vertrauenswürdig erachten, können Sie jedoch auch nicht signierte Pakete einchecken. Diese Pakete werden auf dieselbe Weise wie oben beschrieben gesichert, werden jedoch beim Einchecken von ePolicy Orchestrator signiert.

Digitale Signaturen garantieren, dass Pakete von McAfee stammen oder von Ihnen eingecheckt wurden und dass sie weder manipuliert noch beschädigt wurden. Der Agent vertraut nur Paketdateien, die von ePolicy Orchestrator oder McAfee signiert sind. Dadurch wird verhindert, dass in Ihrem Netzwerk Pakete empfangen werden, die nicht signiert sind oder aus nicht vertrauenswürdigen Quellen stammen.

Paketreihenfolge und Abhängigkeiten

Wenn eine Produktaktualisierung von einer anderen abhängig ist, müssen Sie die Aktualisierungspakete in der erforderlichen Reihenfolge in das Master-Repository einchecken. Wenn beispielsweise Patch 2 auf Patch 1 beruht, müssen Sie Patch 1 vor Patch 2 einchecken. Die Reihenfolge der Pakete kann nach dem Einchecken nicht mehr geändert werden. Sie müssen sie dann entfernen und in der richtigen Reihenfolge erneut einchecken. Wenn Sie ein Paket einchecken, das ein vorhandenes Paket ersetzt, wird das vorhandene Paket automatisch entfernt.

Ausbringen von Produkten und Aktualisierungen

Durch die Repository-Infrastruktur von McAfee ePO können Sie Produkt- und Aktualisierungspakete von einer zentralen Stelle aus in Ihre verwalteten Systeme ausbringen. Obwohl dieselben Repositories verwendet werden, gibt es Unterschiede.

Vergleich von Produktausbringungs- und Aktualisierungspaketen

Produktausbringungspakete	Aktualisierungspakete
Müssen manuell in das Master-Repository eingecheckt werden.	DAT- und Scan-Modul-Aktualisierungspakete können mit einem Abruf-Task automatisch aus der Quellsite kopiert werden. Alle anderen Pakete müssen manuell in das Master-Repository eingecheckt werden.
Können in verteilte Repositories repliziert und mit einem Ausbringungs-Task automatisch auf verwalteten Systemen installiert werden.	Können in verteilte Repositories repliziert und während einer globalen Aktualisierung automatisch auf verwalteten Systemen installiert werden.
Sofern keine globale Aktualisierung für eine Produktausbringung implementiert wird, muss ein Ausbringungs-Task so konfiguriert und geplant werden, dass das Paket von den verwalteten Systemen abgerufen wird.	Sofern keine globale Aktualisierung für eine Produktaktualisierung implementiert wird, muss ein Client-Aktualisierungs-Task konfiguriert und geplant werden, damit das Paket von den verwalteten Systemen abgerufen wird.

Ausbringen und Aktualisieren von Produkten

Gehen Sie zum Verteilen von DAT- und Scan-Modul-Aktualisierungspaketen wie folgt vor.

1. Checken Sie das Aktualisierungspaket mithilfe eines Abruf-Tasks oder manuell in das Master-Repository ein.
2. Führen Sie eine der folgenden Aktionen aus:
   - Wenn Sie die globale Aktualisierung verwenden, sind für Systeme im Netzwerk keine weiteren Aktionen erforderlich. Für Laptop-Systeme, die das Netzwerk verlassen, sollten Sie jedoch einen Aktualisierungs-Task erstellen und planen.
   - Wenn Sie nicht die globale Aktualisierung verwenden, kopieren Sie die Inhalte des Master-Repositories mithilfe eines Replizierungs-Tasks in die verteilten Repositories. Erstellen und planen Sie dann einen Aktualisierungs-Task, mit dem Agenten die Aktualisierung abrufen und auf verwalteten Systemen installieren.

Erstmaliges Konfigurieren der Ausbringungen von Produkten und Aktualisierungen

Gehen Sie wie nachfolgend beschrieben vor, um sicherzustellen, dass Ihre Ausbringungen von Produkten und Aktualisierungen fehlerfrei durchgeführt werden.

Wenn Sie zum ersten Mal Produkte ausbringen, gehen Sie wie folgt vor:

1. Konfigurieren Sie Server-Tasks für den Repository-Abruf und die Repository-Replizierung.
2. Checken Sie Produkt- und Aktualisierungspakete mit dem **Software-Manager** in das Master-Repository ein.
3. Konfigurieren Sie Client-Tasks für Produktausbringung und -aktualisierung.

Ausbringen von Produkten auf verwaltete Systeme mithilfe des Produktausbringungs-Tasks

Sie können Produkte mithilfe des Client-Tasks **Produktausbringung** auf verwaltete Systeme ausbringen.

Diesen Task können Sie für ein einzelnes System oder für Gruppen in der Systemstruktur erstellen.

Aufgaben

- *Konfigurieren des Ausbringungs-Tasks für Gruppen verwalteter Systeme* auf Seite 210
  Sie können den Produktausbringungs-Task so konfigurieren, dass er Produkte auf Gruppen verwalteter Systeme in der Systemstruktur ausbringt.
- *Konfigurieren des Ausbringungs-Tasks zum Installieren von Produkten auf einem verwalteten System* auf Seite 211
  Mithilfe des Produktausbringungs-Tasks können Sie Produkte auf einem einzelnen System ausbringen.

Konfigurieren des Ausbringungs-Tasks für Gruppen verwalteter Systeme

Sie können den Produktausbringungs-Task so konfigurieren, dass er Produkte auf Gruppen verwalteter Systeme in der Systemstruktur ausbringt.

Vorgehensweise

Definitionen zu Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

1. Klicken Sie auf **Menü | Richtlinie | Client-Task-Katalog**, wählen Sie bei **Client-Task-Typen** den Eintrag **McAfee Agent | Produktausbringung** aus, und klicken Sie dann auf **Aktionen | Neuer Task**. Das Dialogfeld **Neuer Task** wird angezeigt.
2. Vergewissern Sie sich, dass **Produktausbringung** ausgewählt ist, und klicken Sie dann auf **OK**.
3. Geben Sie einen Namen für den Task ein, den Sie erstellen möchten, und fügen Sie gegebenenfalls Anmerkungen hinzu.
4. Wählen Sie neben **Zielplattformen** die Typen der Plattform für die Ausbringung aus.
5. Wählen Sie neben **Produkte und Komponenten** Folgendes aus:
   - Wählen Sie in der ersten Dropdown-Liste das gewünschte Produkt aus. Aufgeführt sind diejenigen Produkte, für die Sie bereits ein Paket in das Master-Repository eingecheckt haben. Wenn das Produkt, das Sie ausbringen möchten, nicht hier aufgeführt ist, müssen Sie das Paket dieses Produkts einchecken.
   - Legen Sie als **Aktion** den Wert **Installieren** fest, und wählen Sie dann die **Sprache** des Pakets und den **Zweig** aus.
   - Geben Sie die gewünschten Befehlszeilenoptionen für die Installation in das Textfeld **Befehlszeile** ein. Informationen zu Befehlszeilenoptionen des zu installierenden Produkts finden Sie in der Produktdokumentation.

   
   Sie können auf **+** oder **-** klicken, um Produkte und Komponenten zur angezeigten Liste hinzuzufügen bzw. daraus zu entfernen.
6. Wählen Sie neben **Optionen** aus, ob dieser Task bei jedem Richtlinienerzwingungsvorgang ausgeführt werden soll (nur unter Windows), und klicken Sie auf **Speichern**.
7. Klicken Sie auf **Menü | Systeme | Systemstruktur | Zugewiesene Client-Tasks**, und wählen Sie dann die gewünschte Gruppe in der Systemstruktur aus.
8. Wählen Sie bei **Voreingestellt** den Filter **Produktausbringung (McAfee Agent)** aus.

   Die einzelnen pro ausgewählter Kategorie zugewiesenen Client-Tasks werden im Detailbereich angezeigt.
9. Klicken Sie auf **Aktionen | Neue Client-Task-Zuweisung**. Der **Generator für Client-Task-Zuweisungen** wird angezeigt.

10 Wählen Sie auf der Seite **Task auswählen** bei **Produkt** den Eintrag **McAfee Agent** und bei **Task-Typ** den Eintrag **Produktausbringung** aus, und wählen Sie dann den Task aus, den Sie zum Ausbringen des Produkts erstellt haben.

11 Wählen Sie neben **Tags** die gewünschten Plattformen aus, auf denen Sie die Pakete ausbringen möchten, und klicken Sie dann auf **Weiter**:

- **Diesen Task an alle Computer senden**
- **Diesen Task nur an Computer senden, die die folgenden Kriterien erfüllen** – Verwenden Sie zum Konfigurieren der Kriterien einen der Links mit der Aufschrift **Bearbeiten**.

12 Wählen Sie auf der Seite **Plan** aus, ob die Planung aktiviert ist, legen Sie die Daten für den Zeitplan fest, und klicken Sie dann auf **Weiter**.

13 Überprüfen Sie die Zusammenfassung, und klicken Sie dann auf **Speichern**.

Konfigurieren des Ausbringungs-Tasks zum Installieren von Produkten auf einem verwalteten System

Mithilfe des Produktausbringungs-Tasks können Sie Produkte auf einem einzelnen System ausbringen.

Erstellen Sie einen Client-Task für die Produktausbringung für ein einzelnes System, wenn für dieses System Folgendes erforderlich ist:

- Ein installiertes Produkt, das von den anderen Systemen in derselben Gruppe nicht benötigt wird
- Eine andere Planung als bei den anderen Systemen in der Gruppe, wenn sich ein System beispielsweise in einer anderen Zeitzone als die anderen gleichrangigen Systeme befindet

Vorgehensweise

Definitionen zu Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

1 Klicken Sie auf **Menü** | **Richtlinie** | **Client-Task-Katalog**, wählen Sie bei **Client-Task-Typen** den Eintrag **McAfee Agent** | **Produktausbringung** aus, und klicken Sie dann auf **Aktionen** | **Neuer Task**.

2 Vergewissern Sie sich, dass **Produktausbringung** ausgewählt ist, und klicken Sie dann auf **OK**.

3 Geben Sie einen Namen für den Task ein, den Sie erstellen möchten, und fügen Sie gegebenenfalls Anmerkungen hinzu.

4 Wählen Sie neben **Zielplattformen** die Typen der Plattform für die Ausbringung aus.

5 Wählen Sie neben **Produkte und Komponenten** Folgendes aus:

- Wählen Sie in der ersten Dropdown-Liste ein Produkt aus. Aufgeführt sind diejenigen Produkte, für die Sie bereits ein Paket in das Master-Repository eingecheckt haben. Wenn das Produkt, das Sie ausbringen möchten, nicht hier aufgeführt ist, müssen Sie das Paket dieses Produkts einchecken.
- Legen Sie als **Aktion** den Wert **Installieren** fest, und wählen Sie dann die **Sprache** des Pakets und den **Zweig** aus.
- Geben Sie die Befehlszeilenoptionen für die Installation in das Textfeld **Befehlszeile** ein. Informationen zu Befehlszeilenoptionen des zu installierenden Produkts finden Sie in der Produktdokumentation.



Sie können auf **+** oder - klicken, um Produkte und Komponenten zur angezeigten Liste hinzuzufügen bzw. daraus zu entfernen.

6 Wählen Sie neben **Optionen** aus, ob dieser Task bei jedem Richtlinienerzwingungsvorgang ausgeführt werden soll (nur unter Windows), und klicken Sie dann auf **Speichern**.

7. Klicken Sie auf **Menü | Systeme | Systemstruktur | Systeme**, wählen Sie das System aus, auf dem ein Produkt ausgebracht werden soll, und klicken Sie dann auf **Aktionen | Agent | Tasks auf einem einzelnen System ändern**.
8. Klicken Sie auf **Aktionen | Neue Client-Task-Zuweisung**.
9. Wählen Sie auf der Seite **Task auswählen** bei **Produkt** den Eintrag **McAfee Agent** und bei **Task-Typ** den Eintrag **Produktausbringung** aus, und wählen Sie dann den Task aus, den Sie zum Ausbringen des Produkts erstellt haben.
10. Wählen Sie neben **Tags** die Plattformen aus, auf denen Sie die Pakete ausbringen möchten, und klicken Sie dann auf **Weiter**:
    - **Diesen Task an alle Computer senden**
    - **Diesen Task nur an Computer senden, die die folgenden Kriterien erfüllen** – Verwenden Sie zum Konfigurieren der Kriterien einen der Links mit der Aufschrift **Bearbeiten**.
11. Wählen Sie auf der Seite **Plan** aus, ob die Planung aktiviert ist, legen Sie die Daten für den Zeitplan fest, und klicken Sie dann auf **Weiter**.
12. Überprüfen Sie die Zusammenfassung, und klicken Sie dann auf **Speichern**.

Aktualisierungs-Tasks

Nachdem ein Aktualisierungspaket in das Master-Repository eingecheckt und in die verteilten Repositories repliziert wurde, müssen die Agenten auf den verwalteten Systemen erfahren, wann sie die Aktualisierungen aus den verteilten Repositories abrufen sollen. Wenn Sie die globale Aktualisierung verwenden, ist dies nicht erforderlich.

Sie können Client-Aktualisierungs-Tasks erstellen und festlegen, wann und wie die Aktualisierungspakete von den verwalteten Systemen abgerufen werden. Wenn Sie die globale Aktualisierung nicht verwenden, ist das Erstellen dieser Tasks die einzige Möglichkeit, die Client-Aktualisierung mit ePolicy Orchestrator zu steuern.

Bei Verwendung der globalen Aktualisierung ist dieser Task nicht erforderlich. Sie können dennoch als Absicherung einen täglichen Task erstellen.

Erwägungen beim Erstellen von Client-Aktualisierungs-Tasks

Ziehen Sie beim Planen von Client-Aktualisierungs-Tasks Folgendes in Erwägung:

- Erstellen Sie einen täglichen Client-Aktualisierungs-Task auf der obersten Ebene der Systemstruktur, der von allen Systemen geerbt wird. In großen Unternehmen sollten Sie Zufallsintervalle verwenden, damit weniger Bandbreite in Anspruch genommen wird. Bei großen Netzwerken mit Niederlassungen in verschiedenen Zeitzonen sollte der Task für die einzelnen Systeme zur lokalen Systemzeit ausgeführt werden und nicht für alle Systeme gleichzeitig. Auf diese Weise erreichen Sie eine bessere Lastenverteilung im Netzwerk.
- Wenn Sie Replizierungs-Tasks planen, legen Sie den Task so fest, dass er mindestens eine Stunde nach dem geplanten Replizierungs-Task ausgeführt wird.
- Führen Sie Aktualisierungs-Tasks für DAT- und Scan-Modul-Dateien mindestens einmal täglich aus. Verwaltete Systeme könnten beim Netzwerk abgemeldet sein und den geplanten Task verpassen. Durch häufiges Ausführen des Tasks wird sichergestellt, dass auch diese Systeme die Aktualisierung erhalten.

- Für eine maximale Bandbreiteneffizienz sollten Sie verschiedene geplante Client-Aktualisierungs-Tasks erstellen, mit denen separate Komponenten aktualisiert werden und die zu unterschiedlichen Zeiten ausgeführt werden. So können Sie beispielsweise einen Task erstellen, mit dem nur DAT-Dateien aktualisiert werden, und einen weiteren Task, mit dem DAT- und Scan-Modul-Dateien wöchentlich oder monatlich aktualisiert werden (Scan-Modul-Pakete werden weniger häufig veröffentlicht).
- Erstellen und planen Sie weitere Tasks zum Aktualisieren von Produkten, die nicht den Windows-Agenten verwenden.
- Erstellen Sie einen Task zum Aktualisieren der wichtigsten Workstation-Anwendungen (z. B. VirusScan Enterprise), um zu gewährleisten, dass alle Anwendungen aktualisiert werden. Planen Sie ihn so, dass er täglich oder mehrmals täglich ausgeführt wird.

Regelmäßiges Aktualisieren von verwalteten Systemen mit einem geplanten Aktualisierungs-Task

Sie können Aktualisierungs-Tasks erstellen und konfigurieren. Wenn Sie nicht die globale Aktualisierung verwenden, sollten Sie mithilfe eines täglichen Client-Aktualisierungs-Tasks sicherstellen, dass Ihre Systeme immer über die aktuellsten DAT- und Scan-Modul-Dateien verfügen.

Vorgehensweise

Definitionen zu Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

1. Klicken Sie auf **Menü** | **Richtlinie** | **Client-Task-Katalog**, wählen Sie bei **Client-Task-Typen** den Eintrag **McAfee Agent** | **Aktualisieren** aus, und klicken Sie dann auf **Aktionen** | **Neuer Task**. Das Dialogfeld **Neuer Task** wird angezeigt.
2. Vergewissern Sie sich, dass **Aktualisieren** ausgewählt ist, und klicken Sie dann auf **OK**.
3. Geben Sie einen Namen für den Task ein, den Sie erstellen möchten, und fügen Sie gegebenenfalls Anmerkungen hinzu.
4. Wählen Sie neben **Dialogfeld "Aktualisierung wird ausgeführt"** aus, ob der Benutzer wissen soll, dass eine Aktualisierung stattfindet, und ob er den Vorgang aufschieben darf.
5. Wählen Sie neben **Pakettypen** eine der folgenden Optionen aus, und klicken Sie dann auf **Speichern**:
   - **Alle Pakete**
   - **Ausgewählte Pakete** – Bei Auswahl dieser Option müssen Sie konfigurieren, welche der folgenden Elemente enthalten sein sollen:
     - **Signaturen und Scan-Module**

       
       Wenn Sie beim Konfigurieren einzelner Signaturen und Scan-Module die Option **Scan-Modul** aktivieren und **DAT** deaktivieren, wird beim Aktualisieren des neuen Scan-Moduls auch die neue DAT-Datei automatisch aktualisiert, um einen vollständigen Schutz sicherzustellen.
     - **Patches und Service Packs**
6. Klicken Sie auf **Menü** | **Systeme** | **Systemstruktur** | **Systeme**, wählen Sie das System aus, auf dem die Produktaktualisierung ausgebracht werden soll, und klicken Sie dann auf **Aktionen** | **Agent** | **Tasks auf einem einzelnen System ändern**.

   
   Informationen zum Ausbringen von Produktaktualisierungen auf einer Gruppe von Systemen finden Sie unter *Konfigurieren des Ausbringungs-Tasks für Gruppen verwalteter Systeme*.
7. Klicken Sie auf **Aktionen** | **Neue Client-Task-Zuweisung**. Der **Generator für Client-Task-Zuweisungen** wird angezeigt.

8 Wählen Sie auf der Seite **Task auswählen** bei **Produkt** den Eintrag **McAfee Agent** und bei **Task-Typ** den Eintrag **Produktausbringung** aus, und wählen Sie dann den Task aus, den Sie zum Ausbringen der Produktaktualisierung erstellt haben.

9 Wählen Sie neben **Tags** die gewünschten Plattformen aus, auf denen Sie die Pakete ausbringen möchten, und klicken Sie dann auf **Weiter**:

- **Diesen Task an alle Computer senden**
- **Diesen Task nur an Computer senden, die die folgenden Kriterien erfüllen** – Verwenden Sie zum Konfigurieren der Kriterien einen der Links mit der Aufschrift **Bearbeiten**.

10 Wählen Sie auf der Seite **Plan** aus, ob die Planung aktiviert ist, legen Sie die Daten für den Zeitplan fest, und klicken Sie dann auf **Weiter**.

11 Überprüfen Sie die Zusammenfassung, und klicken Sie dann auf **Speichern**.

Der Task wird zur Liste der Client-Tasks für die Gruppen und Systeme hinzugefügt, auf die er angewendet wurde. Agenten erhalten den neuen Aktualisierungs-Task bei ihrer nächsten Kommunikation mit dem Server. Nach der Aktivierung wird der Task zum nächsten geplanten Zeitpunkt ausgeführt. Jedes System wird aus dem entsprechenden Repository aktualisiert, was davon abhängt, wie die Richtlinien für den Agenten für diesen Client konfiguriert sind.

Bestätigen, dass Clients die neuesten DAT-Dateien verwenden

Überprüfen Sie die Version der DAT-Dateien auf verwalteten Systemen mithilfe von Abfragen.

- Klicken Sie auf **Menü** | **Berichterstellung** | **Abfragen und Berichte**, und wählen Sie in der Liste **Abfragen** den Eintrag **VSE: DAT-Ausbringung** aus. Klicken Sie dann auf **Aktionen | Ausführen.**



Weitere Informationen zu dieser Abfrage finden Sie in der VirusScan Enterprise-Dokumentation.

Testen neuer DAT-Dateien und Scan-Module vor dem Verteilen

Es ist sinnvoll, die DAT- und Scan-Modul-Dateien vor dem Ausbringen im gesamten Unternehmen auf einigen wenigen Systemen zu testen. Sie können Aktualisierungspakete mithilfe des Zweigs **Test** Ihres Master-Repositorys testen.

ePolicy Orchestrator stellt zu diesem Zweck drei Repository-Zweige zur Verfügung.

Definitionen zu Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

Vorgehensweise

1 Erstellen Sie einen geplanten Repository-Abruf-Task, der Aktualisierungspakete in den Zweig **Test** des Master-Repositorys kopiert. Planen Sie ihn so, dass er nach der Veröffentlichung neuer DAT-Dateien ausgeführt wird.

   Weitere Informationen finden Sie unter *Ausbringen von Aktualisierungspaketen mit Abruf- und Replizierungs-Tasks*.

2 Erstellen Sie eine Gruppe, oder wählen Sie in der Systemstruktur eine Gruppe aus, die als Testgruppe dienen soll, und erstellen Sie dann eine McAfee Agent-Richtlinie, nach der die Systeme nur den Zweig **Test** verwenden sollen (im Abschnitt **Repository-Zweig, der für die jeweiligen Aktualisierungstypen verwendet werden soll** auf der Registerkarte **Aktualisierungen**).

   Die Richtlinien werden wirksam, sobald der Agent den Server kontaktiert. Bei der nächsten Aktualisierung ruft der Agent die Aktualisierungen aus dem Zweig **Test** ab. Weitere Informationen finden Sie unter *Konfigurieren des Ausbringungs-Tasks für Gruppen verwalteter Systeme*.

3. Erstellen Sie einen geplanten Client-Aktualisierungs-Task für die Testsysteme, der DAT- und Scan-Modul-Dateien aus dem Zweig **Test** des Repositorys aktualisiert. Planen Sie den Task so, dass er ein oder zwei Stunden nach dem geplanten Beginn des Repository-Abruf-Tasks ausgeführt wird.

   Der erstellte Aktualisierungs-Task zum Testen auf der Ebene der Testgruppe sorgt dafür, dass er nur für diese Gruppe ausgeführt wird. Weitere Informationen finden Sie unter *Regelmäßiges Aktualisieren von verwalteten Systemen mit einem geplanten Aktualisierungs-Task*.

4. Überwachen Sie die Systeme in der Testgruppe so lange, bis Sie mit dem Ergebnis zufrieden sind.

5. Verschieben Sie die Pakete aus dem Zweig **Test** in den Zweig **Aktuell** Ihres Master-Repositorys. Klicken Sie auf **Menü** | **Software** | **Master-Repository**, um die Seite **Master-Repository** zu öffnen.

   Durch Hinzufügen zum Zweig **Aktuell** stehen die Pakete nun Ihrer Produktionsumgebung zur Verfügung. Wenn das nächste Mal ein Client-Aktualisierungs-Task Pakete aus dem Zweig **Aktuell** abruft, werden die neuen DAT- und Scan-Modul-Dateien an die Systeme verteilt, die den Task verwenden. Weitere Informationen finden Sie unter *Manuelles Einchecken von Paketen*.

Verwalten von Client-Tasks

Sie können Client-Tasks erstellen und verwalten.

Aufgaben

- *Erstellen von Client-Tasks* auf Seite 215
  Mithilfe von Client-Tasks können Sie unter anderem Produkt-Software automatisch ausbringen und Produktaktualisierungen durchführen. Dieser Vorgang ist für alle Client-Tasks ähnlich.
- *Bearbeiten von Client-Tasks* auf Seite 216
  Sie können alle zuvor konfigurierten Client-Task-Einstellungen oder Zeitplaninformationen bearbeiten.
- *Löschen von Client-Tasks* auf Seite 216
  Sie können jeden zuvor konfigurierten Client-Task löschen.
- *Vergleichen von Client-Tasks* auf Seite 216
  Mithilfe der Option **Client-Task-Vergleich** können Sie Client-Tasks vergleichen. Auf diese Weise können Sie feststellen, welche Einstellungen identisch und welche unterschiedlich sind.

Erstellen von Client-Tasks

Mithilfe von Client-Tasks können Sie unter anderem Produkt-Software automatisch ausbringen und Produktaktualisierungen durchführen. Dieser Vorgang ist für alle Client-Tasks ähnlich.

In einigen Fällen müssen Sie eine neue Client-Task-Zuweisung erstellen, um einen Client-Task einer Systemstrukturgruppe zuzuordnen.

Vorgehensweise

Definitionen zu Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

1. Klicken Sie auf **Menü** | **Richtlinie** | **Client-Task-Katalog**. Das Dialogfeld **Neuer Task** wird angezeigt. Wählen Sie die gewünschte Gruppe in der Systemstruktur aus, und klicken Sie dann auf **Aktionen** | **Neuer Task**.

   Der **Generator für Client-Tasks** wird geöffnet.

2. Wählen Sie in der Liste einen Task-Typ aus, und klicken Sie dann auf **OK**. Der **Generator für Client-Tasks** wird geöffnet.

   Wählen Sie zum Beispiel **Produktaktualisierung** aus.

3 Geben Sie einen Namen und eine Beschreibung für den zu erstellenden Task ein, und konfigurieren Sie dann die Einstellungen für den neuen Task.



Welche Konfigurationsoptionen zur Verfügung stehen, hängt vom ausgewählten Task-Typ ab.

4 Überprüfen Sie die Task-Einstellungen, und klicken Sie dann auf **Speichern**.

Der Task wird der Liste der Client-Tasks für den ausgewählten Client-Task-Typ hinzugefügt.

Bearbeiten von Client-Tasks

Sie können alle zuvor konfigurierten Client-Task-Einstellungen oder Zeitplaninformationen bearbeiten.

Vorgehensweise

Definitionen zu Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

1. Klicken Sie auf **Menü** | **Richtlinie** | **Client-Task-Katalog**. Das Dialogfeld **Client-Task-Katalog** wird angezeigt.
2. Wählen Sie links in der Navigationsstruktur den **Client-Task-Typ** aus. Die verfügbaren Client-Tasks werden rechts im Fenster angezeigt.
3. Doppelklicken Sie auf den Namen des Client-Tasks. Das Dialogfeld **Client-Task-Katalog** wird mit dem Client-Task angezeigt.
4. Bearbeiten Sie die Task-Einstellungen nach Bedarf, und klicken Sie dann auf **Speichern**.

Die Änderungen werden auf den verwalteten Systemen nach der nächsten Agent-zu-Server-Kommunikation wirksam.

Löschen von Client-Tasks

Sie können jeden zuvor konfigurierten Client-Task löschen.

Vorgehensweise

Definitionen zu Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

1. Klicken Sie auf **Menü** | **Richtlinie** | **Client-Task-Katalog**. Das Dialogfeld **Client-Task-Katalog** wird angezeigt.
2. Wählen Sie links in der Navigationsstruktur den **Client-Task-Typ** aus. Die verfügbaren Client-Tasks werden rechts im Fenster angezeigt.
3. Klicken Sie in der Spalte **Aktionen** neben dem gewünschten Client-Task auf **Löschen**.
4. Klicken Sie auf **OK**.

Vergleichen von Client-Tasks

Mithilfe der Option **Client-Task-Vergleich** können Sie Client-Tasks vergleichen. Auf diese Weise können Sie feststellen, welche Einstellungen identisch und welche unterschiedlich sind.

Viele der auf dieser Seite enthaltenen Werte und Variablen sind produktspezifisch. Informationen zu Optionen, die nicht in der Tabelle aufgeführt sind, finden Sie in der Produktdokumentation des jeweiligen Produkts, von dem der Client-Task stammt, den Sie vergleichen möchten.

Vorgehensweise

Definitionen zu Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

1. Klicken Sie auf **Menü** | **Client-Task-Vergleich**, und wählen Sie dann in den Listen die gewünschten Einstellungen für **Produkt**, **Client-Task-Typ** und **Anzeigen** aus.

   Mit diesen Einstellungen werden die zu vergleichenden Client-Tasks in den Listen **Client-Task 1** und **Client-Task 2** aufgefüllt.

2. Wählen Sie die zu vergleichenden Client-Tasks in der Zeile **Client-Tasks vergleichen** in den Spalten der Listen **Client-Task 1** und **Client Task 2** aus.

   In den beiden obersten Zeilen der Tabelle wird angezeigt, wie viele Einstellungen unterschiedlich und wie viele identisch sind. Wenn weniger Daten angezeigt werden sollen, können Sie auch die Einstellung **Anzeigen** von **Alle Client-Task-Einstellungen** in **Unterschiede zwischen Client-Tasks** oder **Übereinstimmungen zwischen Client-Tasks** ändern.

3. Klicken Sie auf **Drucken**, um eine druckfähige Ansicht des Vergleichs anzuzeigen.

Server-Tasks

Server-Tasks sind konfigurierbare Aktionen, die auf dem ePolicy Orchestrator-Server nach einem Zeitplan ausgeführt werden. Sie können Server-Tasks nutzen, um sich wiederholende Aufgaben zu automatisieren, die auf dem Server durchgeführt werden müssen.

McAfee ePO-Software verfügt standardmäßig über vorkonfigurierte Server-Tasks und Aktionen. Viele zusätzliche Software-Produkte, die mit dem ePolicy Orchestrator-Server verwaltet werden, fügen weitere vorkonfigurierte Server-Tasks hinzu.

Globale Aktualisierung

Durch die globale Aktualisierung wird das Replizieren in die verteilten Repositories automatisiert, und Ihre verwalteten Systeme werden auf dem aktuellsten Stand gehalten. Es sind keine Replizierungs- und Aktualisierungs-Tasks erforderlich. Stattdessen wird durch das Einchecken von Inhalten in das Master-Repository eine globale Aktualisierung ausgelöst. Der gesamte Vorgang nimmt in den meisten Umgebungen nicht länger als eine Stunde in Anspruch.

Sie können außerdem angeben, durch welche Pakete und Aktualisierungen eine globale Aktualisierung ausgelöst wird. Wenn nur bestimmte Inhalte eine globale Aktualisierung auslösen sollen, müssen Sie einen Task erstellen, der alle anderen Inhalte repliziert und verteilt.



Wenn Sie die globale Aktualisierung verwenden, sollten Sie einen regelmäßigen Abruf-Task (zum Aktualisieren des Master-Repositorys) planen, der bei minimaler Netzwerkauslastung ausgeführt wird. Die globale Aktualisierung ist zwar die schnellste Aktualisierungsmethode, verursacht dabei jedoch verstärkten Netzwerkverkehr.

Die globale Aktualisierung

1. Die Inhalte werden in das Master-Repository eingecheckt.
2. Der Server führt eine inkrementelle Replizierung in alle verteilten Repositories durch.
3. Der Server stellt eine SuperAgent-Reaktivierung für alle SuperAgents in der Umgebung aus.
4. Der SuperAgent sendet eine Nachricht über die globale Aktualisierung an alle Agenten in dem SuperAgent-Subnetz.

5. Bei Empfang der Übertragung erhält der Agent eine für die Aktualisierung erforderliche Katalogmindestversion.
6. Der Agent durchsucht die verteilten Repositories nach einer Site, die diese Katalogmindestversion enthält.
7. Sobald er ein passendes Repository gefunden hat, führt er den Aktualisierungs-Task aus.

Wenn der Agent die Übertragung nicht empfängt (z. B. weil der Client-Computer ausgeschaltet ist oder keine SuperAgents vorhanden sind), wird die Katalogmindestversion beim nächsten ASKI übertragen, wodurch der Vorgang initiiert wird.



Wenn der Agent eine Benachrichtigung vom SuperAgent empfängt, erhält er die Liste der aktualisierten Pakete. Wenn der Agent die neue Katalogversion beim nächsten ASKI erhält, verfügt er nicht über die Liste der zu aktualisierenden Pakete und aktualisiert daher alle verfügbaren Pakete.

Voraussetzungen

Folgende Voraussetzungen müssen für das Implementieren der globalen Aktualisierung erfüllt sein:

- Ein SuperAgent muss denselben ASSC-Schlüssel (Schlüssel für sichere Agenten-Server-Kommunikation) wie die Agenten verwenden, die seine Reaktivierung empfangen.
- Auf jedem Übertragungssegment ist ein SuperAgent installiert. Verwaltete Systeme können erst dann eine SuperAgent-Reaktivierung empfangen, wenn sich ein SuperAgent im selben Übertragungssegment befindet. Bei der globalen Aktualisierung wird die SuperAgent-Reaktivierung verwendet, um die Agenten über neu verfügbare Aktualisierungen zu benachrichtigen.
- Verteilte Repositories wurden in Ihrer Umgebung eingerichtet und konfiguriert. SuperAgent-Repositories werden empfohlen, sind jedoch nicht erforderlich. Die globale Aktualisierung funktioniert bei allen Typen von verteilten Repositories.
- Wenn Sie SuperAgent-Repositories verwenden, müssen die verwalteten Systeme das Repository mit den Aktualisierungen erkennen können. Damit Systeme Reaktivierungen empfangen können, muss in jedem Übertragungssegment zwar ein SuperAgent vorhanden sein, SuperAgent-Repositories sind jedoch nicht erforderlich. Jedoch müssen die verwalteten Systeme das SuperAgent-Repository "sehen", von dem aus die Aktualisierung erfolgen soll.

Automatisches Ausbringen von Aktualisierungspaketen per globaler Aktualisierung

Sie können auf dem Server die globale Aktualisierung aktivieren, damit vom Benutzer festgelegte Aktualisierungspakete automatisch auf verwalteten Systemen ausgebracht werden.

Vorgehensweise

Definitionen zu Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

1. Klicken Sie auf **Menü** | **Konfiguration** | **Server-Einstellungen**, wählen Sie **Globale Aktualisierung** aus, und klicken Sie dann unten auf der Seite auf **Bearbeiten**.
2. Wählen Sie auf der Seite **Globale Aktualisierung: Bearbeiten** neben **Status** die Option **Aktiviert** aus.

3. Ändern Sie das **Zufallsintervall** bei Bedarf.

   Jede Client-Aktualisierung wird zu einem zufälligen Zeitpunkt innerhalb dieses Zufallsintervalls durchgeführt, wodurch die Netzwerkbelastung besser verteilt wird. Die Standardeinstellung beträgt **20 Minuten**.

   Wenn Sie zum Beispiel 1.000 Clients mit dem standardmäßigen Zufallsintervall von 20 Minuten aktualisieren, werden in diesem Zeitraum etwa 50 Clients pro Minute aktualisiert, wodurch das Netzwerk und der Server entlastet werden. Ohne die Zufallsgenerierung würden alle 1.000 Clients gleichzeitig aktualisiert werden.

4. Wählen Sie neben **Pakettypen** aus, welche Pakete eine Aktualisierung auslösen.

   Die globale Aktualisierung wird nur dann ausgelöst, wenn für die hier ausgewählten Komponenten neue Pakete in das Master-Repository eingecheckt werden oder in einen anderen Zweig verschoben werden. Wählen Sie die Komponenten daher sorgfältig aus.

   - **Signaturen und Scan-Module** – Wählen Sie **Host Intrusion Prevention-Inhalt** aus, wenn erforderlich.

   Von der Auswahl eines Pakettyps hängt ab, wodurch eine globale Aktualisierung initialisiert wird (nicht, was dabei aktualisiert wird). Agenten erhalten während der globalen Aktualisierung eine Liste von aktualisierten Paketen. Anhand dieser Liste installieren Agenten nur die Aktualisierungen, die erforderlich sind. So aktualisieren Agenten zum Beispiel nicht alle Pakete, sondern nur die, die seit der letzten Aktualisierung geändert wurden.

5. Klicken Sie abschließend auf **Speichern**.

   Nachdem die globale Aktualisierung aktiviert wurde, wird eine Aktualisierung ausgelöst, sobald eines der ausgewählten Pakete eingecheckt oder in einen anderen Zweig verschoben wird.

   Achten Sie darauf, dass ein Task vom Typ "Jetzt abrufen" ausgeführt wird und ein regelmäßiger Server-Task vom Typ "Repository-Abruf" geplant ist, wenn die automatische Aktualisierung fertig konfiguriert ist.

Abruf-Tasks

Abruf-Tasks aktualisieren Ihr Master-Repository mit den DAT- und Scan-Modul-Aktualisierungspaketen aus der Quellsite. DAT- und Scan-Modul-Dateien werden häufig aktualisiert. McAfee veröffentlicht neue DAT-Dateien täglich und Scan-Modul-Dateien etwas seltener. Bringen Sie diese Pakete so schnell wie möglich auf die verwalteten Systeme aus, um diese vor den neuesten Bedrohungen zu schützen.

In dieser Version können Sie festlegen, welche Pakete aus der Quellsite in das Master-Repository kopiert werden sollen.



Extra.DAT-Dateien müssen manuell in das Master-Repository eingecheckt werden. Diese Dateien werden auf der McAfee-Website veröffentlicht.

Ein Server-Task vom Typ "Repository-Abruf" wird automatisch und regelmäßig zu den von Ihnen festgelegten Zeiten ausgeführt. So können Sie beispielsweise einen wöchentlichen Repository-Abruf-Task für jeden Donnerstag um 05:00 Uhr planen.

Sie können den Task "Jetzt abrufen" auch so planen, dass Aktualisierungen sofort in das Master-Repository eingecheckt werden, zum Beispiel wenn McAfee Sie vor einem sich schnell ausbreitenden Virus warnt und zum Schutz vor diesen Virus eine neue DAT-Datei veröffentlicht.

Wenn ein Abruf-Task fehlschlägt, müssen Sie die Pakete manuell in das Master-Repository einchecken.

Nach dem Aktualisieren des Master-Repositorys können Sie diese Aktualisierungen mit Replizierungs-Tasks oder über die globale Aktualisierung automatisch in Ihren Systemen verteilen.

Erwägungen beim Planen von Abruf-Tasks

Berücksichtigen Sie beim Planen von Abruf-Tasks Folgendes:

- **Auslastung von Bandbreite und Netzwerk** – Wenn Sie (wie empfohlen) die globale Aktualisierung verwenden, sollten Sie die Ausführung von Abruf-Tasks für Zeiten planen, zu denen das Netzwerk nicht so sehr von anderen Ressourcen in Anspruch genommen wird. Bei der globalen Aktualisierung werden die Aktualisierungsdateien automatisch verteilt, sobald der Abruf-Task abgeschlossen ist.
- **Häufigkeit des Tasks** – DAT-Dateien werden täglich veröffentlicht, was Sie aber möglicherweise nicht täglich in Anspruch nehmen möchten.
- **Replizierungs- und Aktualisierungs-Tasks** – Planen Sie Replizierungs- und Client-Aktualisierungs-Tasks, um sicherzustellen, dass alle Aktualisierungsdateien in Ihrer Umgebung verteilt werden.

Replizierungs-Tasks

Verwenden Sie Replizierungs-Tasks zum Kopieren von Inhalten des Master-Repositorys in verteilte Repositories. Replizieren Sie Inhalte im Master-Repository in alle verteilten Repositories. Andernfalls können diese Aktualisierungen von einigen Systemen nicht empfangen werden. Stellen Sie sicher, dass alle verteilten Repositories aktuell sind.



Wenn Sie alle Aktualisierungen global vornehmen, sind Replizierungs-Tasks für Ihre Umgebung unter Umständen nicht erforderlich. Allerdings werden sie zur Absicherung empfohlen. Wenn Sie Aktualisierungen dagegen generell nicht global vornehmen, müssen Sie einen Server-Task vom Typ "Repository-Replizierung" planen oder einen Task vom Typ "Jetzt replizieren" ausführen.

Um zu gewährleisten, dass die verteilten Repositories auf dem neuesten Stand sind, sollten Sie regelmäßige Server-Tasks zur Repository-Replizierung planen. Mit dem Planen von täglichen Replizierungs-Tasks stellen Sie sicher, dass die verwalteten Systeme aktuell bleiben. Automatisieren Sie die Replizierung in Ihre verteilten Repositories, indem Sie Repository-Replizierungs-Tasks verwenden.

Gelegentlich müssen Sie an Ihrem Master-Repository Änderungen vornehmen, die Sie sofort in Ihren verteilten Repositories replizieren möchten, statt auf die nächste geplante Replizierung zu warten. Führen Sie in diesem Fall einen Task "Jetzt replizieren" aus, um Ihre verteilten Repositories manuell zu aktualisieren.

Vergleich von vollständiger und inkrementeller Replizierung

Wählen Sie beim Erstellen eines Replizierungs-Tasks für die Replizierung **Inkrementell** oder **Vollständig** aus. Bei inkrementeller Replizierung werden nur die neuen Aktualisierungen im Master-Repository kopiert, die sich noch nicht im verteilten Repository befinden. Dadurch sinkt die Netzwerkbelastung. Bei einer vollständigen Replizierung wird der gesamte Inhalt des Master-Repositorys kopiert.



Es wird empfohlen, einen täglichen inkrementellen Replizierungs-Task zu planen. Wenn Dateien im verteilten Repository außerhalb der ePolicy Orchestrator-eigenen Replizierungsfunktion gelöscht werden können, planen Sie einen wöchentlichen Task für eine vollständige Replizierung.

Repository-Auswahl

Neue verteilte Repositories werden zur Repository-Listen-Datei hinzugefügt, die alle verfügbaren verteilten Repositories enthält. Die Agenten der verwalteten Systeme aktualisieren diese Datei bei

jeder Kommunikation mit dem McAfee ePO-Server. Bei jedem Start des Agenten-Dienstes (**McAfee Framework-Dienst**) und bei Änderungen der Repository-Liste wird ein Repository vom Agenten ausgewählt.

Durch die selektive Replizierung kann die Aktualisierung einzelner Repositories besser gesteuert werden. Wenn Sie Replizierungs-Tasks planen, haben Sie folgende Möglichkeiten:

- Wählen Sie bestimmte verteilte Repositories, auf die der Task angewendet werden soll. Durch das Replizieren auf verschiedene verteilte Repositories zu unterschiedlichen Uhrzeiten wird die erforderliche Bandbreite reduziert. Diese Repositories können beim Erstellen oder Bearbeiten des Replizierungs-Tasks angegeben werden.
- Wählen Sie bestimmte Dateien und Signaturen, die auf verteilte Repositories repliziert werden sollen. Wenn Sie auswählen, welche Dateitypen für jedes System erforderlich sind, das sich in das verteilte Repository eincheckt, wird die erforderliche Bandbreite reduziert. Wenn Sie Ihre verteilten Repositories definieren oder bearbeiten, können Sie festlegen, welche Pakete in das verteilte Repository repliziert werden sollen.



Diese Funktion ist für das Aktualisieren von Produkten gedacht, die nur auf einem Teil der Systeme in Ihrer Umgebung installiert sind, z. B. VirusScan Enterprise. Mithilfe der Funktion können Sie diese Aktualisierungen auf die verteilten Repositories beschränken, die diese Systeme verwenden.

Auswählen von Repositories durch Agenten

Standardmäßig können Agenten versuchen, Aktualisierungen von jedem Repository in der Repository-Listen-Datei durchzuführen. Agenten können mithilfe einer Netzwerk-ICMP-Ping-Abfrage oder einem Subnetzadressen-Vergleichsalgorithmus das verteilte Repository mit der kürzesten Reaktionszeit suchen. Meist ist dies das verteilte Repository, das sich im Netzwerk dem System am nächsten befindet.

Wenn Sie verteilte Repositories in der Agenten-Richtlinie aktivieren oder deaktivieren, können Sie steuern, welche verteilten Repositories die Agenten zum Aktualisieren verwenden. Sie sollten Repositories in den Richtlinieneinstellungen jedoch nicht deaktivieren. Wenn die Agenten sich über ein beliebiges verteiltes Repository aktualisieren können, wird gewährleistet, dass sie die Aktualisierungen erhalten.

Zulässige Cron-Syntax beim Planen von Server-Tasks

Die Cron-Syntax besteht aus sechs oder sieben Feldern, getrennt durch ein Leerzeichen. Zulässige Cron-Syntax wird, nach Feldern in absteigender Reihenfolge, in der folgenden Tabelle aufgeführt. Die meisten Cron-Syntaxen sind zulässig, einige wenige Fälle werden jedoch nicht unterstützt. Sie können beispielsweise nicht gleichzeitig Werte für den Wochentag und den Tag des Monats angeben.

Feldname	Zulässige Werte	Zulässige Sonderzeichen
Sekunden	0–59	, - * /
Minuten	0–59	, - * /
Stunden	0–23	, - * /
Tag des Monats	1–31	, - * ? / L W C
Monat	1–12 oder JAN – DEC	, - * /
Wochentag	1–7 oder SUN – SAT	, - * ? / L C #
Jahr (optional)	Leer oder 1970–2099	, - * /

Hinweise zu zulässigen Sonderzeichen

- Kommas (,) sind zulässig, um weitere Werte anzugeben. Beispiel: "`5,10,30`" oder "`MON,WED,FRI`".
- Sternchen (*) werden für die Angabe "jede" verwendet. So bedeutet zum Beispiel "`*`" im Feld **Minuten** "jede Minute".
- Fragezeichen (?) sind zulässig, um keinen spezifischen Wert für den Wochentag oder den Tag im Monat anzugeben.

  Sie müssen das Fragezeichen in einem der Felder verwenden, können es jedoch nicht gleichzeitig in beiden Feldern verwenden.

- Schrägstriche (/) kennzeichnen Inkremente. So bedeutet zum Beispiel "`5/15`" im Feld **Minuten**, dass der Task in der 5., 20., 35. und 50. Minute ausgeführt wird.
- Der Buchstabe "L" bedeutet "letzter" in den Feldern **Wochentag** und **Tag des Monats**. So bedeutet zum Beispiel "`0 15 10 ? * 6L`": der letzte Freitag jeden Monats um 10:15 Uhr.
- Der Buchstabe "W" steht für "Wochentag". Wenn Sie also als Tag des Monats "`15W`" erstellt haben, bezeichnet dies den Wochentag, der dem 15. des Monats am nächsten liegt. Sie können auch "`LW`" angeben, was für den letzten Wochentag des Monats steht.
- Das Rautenzeichen "#" kennzeichnet den "n-ten" Tag des Monats. So steht zum Beispiel "`6#3`" im Feld **Wochentag** für den dritten Freitag jeden Monats, "`2#1`" für den ersten Montag und "`4#5`" für den fünften Mittwoch.

  Wenn es im jeweiligen Monat keinen fünften Mittwoch gibt, wird der Task nicht ausgeführt.

Anzeigen von Informationen zu Abruf- und Replizierungs-Tasks im Server-Task-Protokoll

Im Server-Task-Protokoll finden Sie neben allen Server-Tasks auch Informationen zu den Abruf- und Replizierungs-Tasks. Dem Protokoll können Sie den Status des jeweiligen Tasks und eventuelle Fehler entnehmen.

- Gehen Sie wie hier beschrieben vor, um auf die Informationen zu Abruf- und Replizierungs-Tasks zuzugreifen: Klicken Sie auf **Menü** | **Automatisierung** | **Server-Task-Protokoll**.

  Die folgenden Informationen zu Replizierungs-Tasks werden angezeigt:

  - Startdatum und Task-Dauer
  - Task-Status für jede Site (wenn erweitert)
  - Eventuelle Fehler und Warnungen (und deren Codes) und für welche Site sie gelten

  Die folgenden Informationen zu Abruf-Tasks werden angezeigt:

  - Startdatum und Task-Dauer
  - Fehler oder Warnungen und die zugehörigen Codes
  - Status der einzelnen Pakete, die in das Master-Repository eingecheckt werden
  - Informationen zu neuen Paketen, die in das Master-Repository eingecheckt werden

Konfigurieren von Product Improvement Program

Mit McAfee Product Improvement Program können McAfee-Produkte weiter verbessert werden. Es erfasst proaktiv und in regelmäßigen Abständen Daten auf den vom ePolicy Orchestrator-Server verwalteten Client-Systemen.

McAfee Product Improvement Program erfasst Daten zu den folgenden Aspekten:

- Systemumgebung (Software- und Hardware-Details)
- Effektivität von installierten McAfee-Produktfunktionen
- McAfee-Produktfehler und zugehörige Windows-Ereignisse

Vorgehensweise

Definitionen zu Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

1. Klicken Sie auf **Menü** | **Konfiguration** | **Server-Einstellungen**, wählen Sie in der Liste **Einstellungskategorien** den Eintrag **Product Improvement Program** aus, und klicken Sie dann auf **Bearbeiten**.
2. Wählen Sie **Ja** aus, um McAfee das Erfassen anonymer Diagnose- und Nutzungsdaten zu erlauben, und klicken Sie dann auf **Speichern**.



Klicken Sie hier, wenn Sie mehr über McAfee Product Improvement Program erfahren möchten.

15 Manuelle Verwaltung von Paketen und Aktualisierungen

Wenn Sie neue Produkte außerhalb ihrer normalen geplanten Task-Routinen ausbringen möchten, können Sie diese manuell einchecken.

Inhalt

Hinzufügen von Produkten zur Verwaltung

Die Erweiterung für ein Produkt muss installiert werden, damit dieses Produkt von ePolicy Orchestrator verwaltet werden kann.

Bevor Sie beginnen

Vergewissern Sie sich, dass sich die Erweiterungsdatei in einem Speicherort auf dem Netzwerk befindet, auf den zugegriffen werden kann.

Vorgehensweise

Definitionen zu Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

1 Klicken Sie in der ePolicy Orchestrator-Konsole auf **Menü** | **Software** | **Erweiterungen** | **Erweiterung installieren**.



Das Master-Repository darf nicht durch mehrere Tasks gleichzeitig aktualisiert werden. Wenn Sie versuchen, während einer Aktualisierung des Master-Repositorys eine Erweiterung zu installieren, wird die folgende Fehlermeldung angezeigt:

Die Erweiterung kann nicht installiert werden. com.mcafee.core.cdm.CommandException: Das ausgewählte Paket kann während eines Abruf-Tasks nicht eingecheckt werden.

Warten Sie, bis die Aktualisierung des Master-Repositorys abgeschlossen ist, und versuchen Sie dann erneut, die Erweiterung zu installieren.

2 Wechseln Sie zur Erweiterungsdatei, wählen Sie sie aus, und klicken Sie auf **OK**.

3 Überprüfen Sie, ob der Produktname in der Liste **Erweiterungen** angezeigt wird.

Manuelles Einchecken von Paketen

Sie können Ausbringungspakete manuell in das Master-Repository einchecken, damit sie von ePolicy Orchestrator ausgebracht werden können.

Vorgehensweise

Definitionen zu Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

1. Klicken Sie auf **Menü** | **Software** | **Master-Repository**, und klicken Sie dann auf **Aktionen** | **Paket einchecken**.

   Der Assistent **Paket einchecken** wird geöffnet.

2. Wählen Sie den Pakettyp aus, wechseln Sie dann zur gewünschten Paketdatei, und wählen Sie sie aus.

3. Klicken Sie auf **Weiter**.

   Die Seite **Paketoptionen** wird angezeigt.

4. Bestätigen oder konfigurieren Sie Folgendes:

   - **Paketinfo** – Bestätigen Sie, dass dies das richtige Paket ist.
   - **Zweig** – Wählen Sie den gewünschten Zweig aus. Wenn in Ihrer Umgebung neue Pakete vor dem Ausbringen in die Produktionsumgebung getestet werden müssen, sollten Sie beim Einchecken von Paketen den Zweig **Test** verwenden. Nachdem Sie die Pakete getestet haben, können Sie sie in den Zweig **Aktuell** verschieben, indem Sie auf **Menü** | **Software** | **Master-Repository** klicken.
   - **Optionen** – Wählen Sie eine der weiteren folgenden Optionen aus:
     - **Vorhandenes Paket in den Zweig "Vorherige" verschieben** – Bei Auswahl dieser Option werden Pakete im Master-Repository aus dem Zweig **Aktuell** in den Zweig **Vorherige** verschoben, wenn ein neueres Paket desselben Typs eingecheckt wird. Diese Option ist nur verfügbar, wenn Sie unter **Zweig** die Option **Aktuell** auswählen.
   - **Paket-Signatur** – Gibt an, ob das Paket von McAfee oder einem Drittanbieter stammt.

5. Klicken Sie auf **Speichern**, um mit dem Einchecken des Pakets zu beginnen, und warten Sie dann, während das Paket eingecheckt wird.

Das neue Paket wird auf der Registerkarte **Master-Repository** in der Liste **Pakete im Master-Repository** angezeigt.

Löschen von DAT- oder Scan-Modul-Paketen aus dem Master-Repository

Sie können DAT- oder Scan-Modul-Pakete aus dem Master-Repository löschen. Wenn Sie regelmäßig neue Aktualisierungspakete einchecken, ersetzen diese die älteren Versionen oder verschieben sie in den Zweig **Vorherige**, sofern Sie den Zweig **Vorherige** verwenden.

Vorgehensweise

Definitionen zu Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

1. Klicken Sie auf **Menü** | **Software** | **Master-Repository**.

   Die Tabelle **Pakete im Master-Repository** wird angezeigt.

2. Klicken Sie in der Zeile mit dem gewünschten Paket auf **Löschen**.

   Das Dialogfeld **Paket löschen** wird angezeigt.

3 Klicken Sie auf **OK**.

Manuelles Verschieben von DAT- und Scan-Modul-Paketen zwischen Zweigen

Sie können Pakete nach dem Einchecken in das Master-Repository manuell zwischen den Zweigen **Test**, **Aktuell** und **Vorherige** verschieben.

Vorgehensweise

Definitionen zu Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

1. Klicken Sie auf **Menü | Software | Master-Repository**.
2. Klicken Sie in der Zeile des gewünschten Pakets auf **Zweig wechseln**.
3. Wählen Sie aus, ob Sie das Paket in einen anderen Zweig verschieben oder kopieren möchten.
4. Wählen Sie aus, welcher Zweig das Paket erhalten soll.

   Wenn Sie in Ihrem Netzwerk mit McAfee® NetShield® for NetWare arbeiten, aktivieren Sie **NetShield for NetWare unterstützen**.

5. Klicken Sie auf **OK**.

Manuelles Einchecken von Scan-Modul-, DAT- und Extra.DAT-Aktualisierungspaketen

Sie können Aktualisierungspakete manuell in das Master-Repository einchecken, damit sie anschließend mithilfe von ePolicy Orchestrator ausgebracht werden können. Einige Pakete können nur manuell eingecheckt werden.

Vorgehensweise

Definitionen zu Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

1. Klicken Sie auf **Menü | Software | Master-Repository**, und klicken Sie dann auf **Aktionen | Paket einchecken**.

   Der Assistent **Paket einchecken** wird geöffnet.

2. Wählen Sie den Pakettyp aus, wechseln Sie dann zur gewünschten Paketdatei, und wählen Sie sie aus.
3. Klicken Sie auf **Weiter**.

   Die Seite **Paketoptionen** wird angezeigt.

4. Wählen Sie einen Zweig aus:
   - **Aktuell** – Hiermit werden die Pakete ohne vorherigen Test verwendet.
   - **Test** – Hiermit werden die Pakete zuvor in einer Testumgebung getestet.

     Nachdem Sie die Pakete getestet haben, können Sie sie in den Zweig **Aktuell** verschieben, indem Sie auf **Menü | Software | Master-Repository** klicken.

   - **Vorherige** – Hiermit wird das Paket mithilfe der vorherigen Version empfangen.

5 Wählen Sie neben **Optionen** Folgendes aus:

- **Vorhandenes Paket in den Zweig "Vorherige" verschieben** – Wählen Sie diese Option aus, um das vorhandene Paket (vom selben Typ wie das, das Sie einchecken) in den Zweig **Vorherige** zu verschieben.

6 Klicken Sie auf **Speichern**, um mit dem Einchecken des Pakets zu beginnen. Warten Sie, während das Paket eingecheckt wird.

Das neue Paket wird auf der Seite **Master-Repository** in der Liste **Pakete im Master-Repository** angezeigt.

16 Ereignisse und Antworten

Sie können den McAfee ePO-Server so konfigurieren, dass bei Bedrohungs-, Client- oder Server-Ereignissen eine Antwort ausgelöst wird.

Inhalt

Verwenden automatischer Antworten

Für welche Ereignistypen Sie automatische Antworten konfigurieren können, hängt davon ab, welche Software-Produkte mit dem ePolicy Orchestrator-Server verwaltet werden.

In der Standardeinstellung kann eine Antwort folgende Aktionen beinhalten:

- Das Erstellen von Problemen
- Das Ausführen von Server-Tasks
- Das Ausführen externer Befehle
- Das Ausführen von Systembefehlen
- Das Senden von E-Mail-Nachrichten
- Das Senden von SNMP-Traps

Es lässt sich genau konfigurieren, bei welchen Ereignissen aus welchen Kategorien Benachrichtigungen generiert und mit welcher Häufigkeit diese Benachrichtigungen gesendet werden sollen.

Diese Funktion dient dazu, benutzerdefinierte Benachrichtigungen und Aktionen für die Fälle zu erstellen, in denen die Bedingungen einer Regel erfüllt sind. Zu diesen Bedingungen gehören u. a.:

- Die Erkennung von Bedrohungen durch Ihre Antiviren-Software. Es werden zwar viele Antivirenprodukte unterstützt, bei VirusScan Enterprise jedoch beinhalten Ereignisse auch die IP-Adresse der Angriffsquelle, sodass das System, das die übrige Umgebung infiziert, isoliert werden kann.
- Virenausbruch. Zum Beispiel, wenn innerhalb von fünf Minuten 1.000 Ereignisse vom Typ "Virus entdeckt" empfangen werden.
- Hohe Übereinstimmung mit ePolicy Orchestrator-Server-Ereignissen. Zum Beispiel ein Fehler bei einer Repository-Aktualisierung oder einem Replizierungs-Task.

Zusammenspiel der Funktion für automatische Antworten mit der Systemstruktur

Bevor Sie mit dem Planen der Implementierung von automatischen Antworten beginnen, sollten Sie genau verstehen, wie diese Funktion im Zusammenhang mit der Systemstruktur arbeitet.



Diese Funktion hält nicht das beim Erzwingen von Richtlinien verwendete Vererbungsmodell ein.

Automatische Antworten verwenden Ereignisse, die auf Systemen in der Umgebung auftreten, die an den Server übermittelt werden und Antwortregeln ausgelöst haben, die der Gruppe mit den betroffenen Systemen und den übergeordneten Elementen zugeordnet sind. Wenn die Bedingungen einer dieser Regeln erfüllt sind, werden gemäß der Konfiguration der Regel vorher festgelegte Aktionen ausgeführt.

Auf diese Weise können Sie unabhängige Regeln auf unterschiedlichen Ebenen der Systemstruktur konfigurieren. Folgende Eigenschaften können sich für diese Regeln unterscheiden:

- **Schwellenwerte für das Senden einer Benachrichtigung**. So möchte zum Beispiel ein Administrator einer bestimmten Gruppe benachrichtigt werden, wenn innerhalb von 10 Minuten auf 100 Systemen in der Gruppe Viren entdeckt werden, ein anderer Administrator jedoch erst, wenn dies im selben Zeitraum in der gesamten Umgebung auf mindestens 1.000 Systemen geschieht.
- **Empfänger der Benachrichtigung**. Ein Administrator einer bestimmten Gruppe möchte beispielsweise nur dann eine Benachrichtigung erhalten, wenn eine bestimmte Anzahl von Virusentdeckungen in der Gruppe auftritt. Oder ein Administrator möchte, dass alle Gruppenadministratoren eine Benachrichtigung erhalten, wenn eine bestimmte Anzahl von Virusentdeckungen in der gesamten Systemstruktur auftritt.



Server-Ereignisse werden nicht nach dem Speicherort in der Systemstruktur gefiltert.

Beschränkung, Aggregation und Gruppierung

Durch Festlegen von Schwellenwerten, die auf Aggregation, Beschränkung und Gruppierung basieren, können Sie konfigurieren, wann Benachrichtigungen gesendet werden.

Aggregation

Mit der Aggregation können Sie Schwellenwerte für Ereignisse festlegen, ab denen die Regel eine Benachrichtigung sendet. Konfigurieren Sie eine Regel zum Beispiel so, dass eine Benachrichtigung gesendet wird, wenn der Server innerhalb einer Stunde 1.000 Virusentdeckungen von unterschiedlichen Systemen oder 100 Virusentdeckungen von einem System empfängt.

Beschränkung

Wenn Sie eine Regel konfiguriert haben, nach der Sie bei einem möglichen Virenausbruch benachrichtigt werden, können Sie mit der Beschränkung sicherstellen, dass Sie nicht zu viele Benachrichtigungen erhalten. Als Administrator eines umfangreichen Netzwerks erhalten Sie möglicherweise Zehntausende Ereignisse innerhalb einer Stunde, was bei einer solchen Regel zu Tausenden von Benachrichtigungen führen würde. Mithilfe von Antworten können Sie die Anzahl der Benachrichtigungen beschränken, die Sie aufgrund einer einzelnen Regel erhalten. Sie können beispielsweise in derselben Regel bestimmen, dass Sie lediglich eine Benachrichtigung pro Stunde erhalten möchten.

Gruppierung

Mittels Gruppierung können Sie mehrere aggregierte Ereignisse zusammenfassen. So können zum Beispiel Ereignisse mit dem gleichen Schweregrad in einer einzigen Gruppe zusammengefasst werden. Durch eine Gruppierung kann der Administrator auf alle Ereignisse mit diesem oder einem höheren Schweregrad gleichzeitig reagieren. Außerdem können Sie damit auch für die bei verwalteten Systemen oder Servern generierten Ereignisse Prioritäten vergeben.

Standardregeln

Sie können die ePolicy Orchestrator-Standardregeln aktivieren, um die Funktion zum Ausprobieren sofort verwenden zu können.

Vor dem Aktivieren von Standardregeln sollten Sie die folgenden Schritte ausführen:

- Geben Sie den E-Mail-Server an (unter **Menü | Konfiguration | Server-Einstellungen**), von dem die Benachrichtigungsmeldungen gesendet werden.
- Vergewissern Sie sich, dass Sie die E-Mail-Adresse der Person angeben, die E-Mail-Benachrichtigungen empfangen soll. Diese Adresse wird im Assistenten auf der Seite **Aktionen** festgelegt.

Standardbenachrichtigungsregeln

Regelname	Zugehörige Ereignisse	Konfigurationen
Fehler beim Aktualisieren oder Replizieren des verteilten Repositorys	Fehler beim Aktualisieren oder Replizieren des verteilten Repositorys	Sendet eine Benachrichtigung, wenn bei einer Aktualisierung oder einer Replizierung ein Fehler auftritt.
Malware entdeckt	Ereignisse von unbekannten Produkten	Sendet eine Benachrichtigung: • Die Anzahl der Ereignisse erreicht innerhalb einer Stunde mindestens den Wert 1.000. • Eine Benachrichtigung wird max. alle zwei Stunden gesendet. • Sofern vorhanden und zusammen mit vielen anderen Parametern werden die IP-Adresse des Quellsystems, die Bezeichnung für die aktuelle Bedrohung und Informationen zum aktuellen Produkt mitgesendet. • Die Anzahl ausgewählter eindeutiger Werte beträgt 500.
Fehler beim Aktualisieren oder Replizieren des Master-Repositorys	Fehler beim Aktualisieren oder Replizieren des Master-Repositorys	Sendet eine Benachrichtigung, wenn bei einer Aktualisierung oder einer Replizierung ein Fehler auftritt.
Nicht konformer Computer entdeckt	Ereignisse vom Typ **Nicht konformer Computer entdeckt**	Sendet eine Benachrichtigung, wenn ein Ereignis vom Server-Task "Compliance-Ereignis generieren" empfangen wird.

Planen von Antworten

Wenn Sie die folgenden Punkte gut planen, bevor Sie Benachrichtigungsregeln erstellen, können Sie Zeit sparen.

Stellen Sie sicher, dass Sie über einen Plan zu den folgenden Punkten verfügen:

- Ereignistypen und -gruppen (Produkt und Server), die in Ihrer Umgebung Benachrichtigungen auslösen.
- Wer sollte welche Benachrichtigungen erhalten? So ist es zum Beispiel nicht notwendig, den Administrator von Gruppe B über eine fehlgeschlagene Replizierung in Gruppe A zu informieren, es sollten aber alle Administratoren informiert werden, wenn in Gruppe A eine infizierte Datei entdeckt wurde.
- Welche Arten und Ebenen von Grenzwerten möchten Sie für jede Regel festlegen? Eventuell möchten Sie zum Beispiel während eines Virenausbruchs nicht bei jeder infizierten Datei eine E-Mail-Benachrichtigung erhalten. Stattdessen können Sie auswählen, dass Ihnen eine solche Benachrichtigung unabhängig von der Anzahl der vom Server empfangenen Ereignisse höchstens alle fünf Minuten zugesendet wird.
- Welche Befehle oder registrierten ausführbaren Dateien sollen ausgeführt werden, wenn die Bedingungen einer Regel erfüllt sind?
- Welcher Server-Task soll ausgeführt werden, wenn die Bedingungen einer Regel erfüllt sind?

Erstmaliges Konfigurieren von Antworten

Gehen Sie wie nachfolgend allgemein beschrieben vor, wenn Sie zum ersten Mal Ereignisse und automatische Antworten konfigurieren.

Wenn Sie zum ersten Mal eine Regel für automatische Antworten erstellen, sollten Sie die folgenden Punkte beachten:

1. Machen Sie sich mit automatischen Antworten und deren Funktionsweise in der Systemstruktur und im Netzwerk vertraut.
2. Planen Sie die Implementierung. Welche Benutzer müssen über welche Ereignisse informiert werden?
3. Bereiten Sie die Komponenten und Berechtigungen vor, die im Zusammenhang mit automatischen Antworten benötigt werden. Dazu gehören:
   - **Berechtigungen für automatische Antworten** – Erstellen oder bearbeiten Sie Berechtigungssätze, und stellen Sie sicher, dass diese den entsprechenden McAfee ePO-Benutzern zugewiesen sind.
   - **E-Mail-Server** – Konfigurieren Sie den E-Mail-Server (SMTP) unter **Server-Einstellungen**.
   - **Liste der E-Mail-Kontakte** – Geben Sie unter **Kontakte** die Liste an, aus der Sie Empfänger für Benachrichtigungen auswählen.
   - **Registrierte ausführbare Dateien** – Geben Sie eine Liste mit registrierten ausführbaren Dateien an, die ausgeführt werden sollen, wenn die Bedingungen einer Regel erfüllt sind.
   - **Server-Tasks** – Erstellen Sie Server-Tasks, die infolge einer Antwortregel als Aktion ausgeführt werden sollen.
   - **SNMP-Server** – Geben Sie eine Liste von SNMP-Servern an, die beim Erstellen von Regeln verwendet werden sollen. Sie können Regeln konfigurieren, um SNMP-Traps an SNMP-Server zu senden, wenn die Bedingungen zum Erstellen einer Benachrichtigung erfüllt sind.

Bestimmen, wie Ereignisse weitergeleitet werden

Gehen Sie wie in diesen Aufgaben beschrieben vor, um festzulegen, wann Ereignisse weitergeleitet und welche Ereignisse sofort weitergeleitet werden sollen.

Der Server empfängt Ereignisbenachrichtigungen von McAfee Agents. Sie können Agenten-Richtlinien so konfigurieren, dass Ereignisse entweder sofort oder nur in Agent-zu-Server-Kommunikationsintervallen zum Server gesendet werden.

Wenn Sie auswählen, dass Ereignisse sofort gesendet werden sollen (Standard), leitet der Agent alle Ereignisse sofort bei Erhalt weiter.



Das Standardintervall für die Verarbeitung von Ereignisbenachrichtigungen beträgt eine Minute. Daher kann es zu einer Verzögerung kommen, bevor Ereignisse verarbeitet werden. Das Standardintervall können Sie in den Server-Einstellungen für Ereignisbenachrichtigungen (**Menü** | **Konfiguration** | **Server-Einstellungen**) ändern.

Wenn nicht alle Ereignisse sofort gesendet werden sollen, leitet der Agent nur solche Ereignisse unverzüglich weiter, die vom ausstellenden Produkt mit einer hohen Priorität gekennzeichnet wurden. Andere Ereignisse werden nur bei der Agent-zu-Server-Kommunikation gesendet.

Aufgaben

- *Bestimmen der sofort weiterzuleitenden Ereignisse* auf Seite 233
  Legen Sie fest, ob Ereignisse unverzüglich oder nur bei Agent-zu-Server-Kommunikationen weitergeleitet werden sollen.
- *Bestimmen der weiterzuleitenden Ereignisse* auf Seite 234
  Mithilfe der **Server-Einstellungen** können Sie bestimmen, welche Ereignisse an den Server weitergeleitet werden.

Bestimmen der sofort weiterzuleitenden Ereignisse

Legen Sie fest, ob Ereignisse unverzüglich oder nur bei Agent-zu-Server-Kommunikationen weitergeleitet werden sollen.

Wenn für die aktuell angewendete Richtlinie nicht festgelegt ist, dass Ereignisse sofort hochzuladen sind, müssen Sie entweder die aktuell angewendete Richtlinie ändern oder eine neue McAfee Agent-Richtlinie erstellen. Diese Einstellung ist auf der Seite **Bedrohungsereignisprotokoll** konfiguriert.

Definitionen zu Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

Vorgehensweise

1. Klicken Sie auf **Menü** | **Richtlinie** | **Richtlinienkatalog**, und wählen Sie dann in der Dropdown-Liste **Produkt** den Eintrag **McAfee Agent** und in der Dropdown-Liste **Kategorie** den Eintrag **Allgemein** aus.
2. Klicken Sie auf eine vorhandene Agenten-Richtlinie.
3. Aktivieren Sie auf der Registerkarte **Ereignisse** die Option **Weiterleiten von Ereignissen nach Priorität aktivieren**.
4. Wählen Sie den Ereignisschweregrad aus.

   Ereignisse des ausgewählten Schweregrades (und höher) werden sofort an den Server weitergeleitet.
5. Geben Sie ein **Intervall zwischen Uploads** (in Minuten) ein, um die Häufigkeit des anfallenden Datenverkehrs zu regulieren.
6. Geben Sie die **Maximale Anzahl von Ereignissen pro Upload** ein, um den Umfang des anfallenden Datenverkehrs zu begrenzen.
7. Klicken Sie auf **Speichern**.

Bestimmen der weiterzuleitenden Ereignisse

Mithilfe der **Server-Einstellungen** können Sie bestimmen, welche Ereignisse an den Server weitergeleitet werden.

Definitionen zu Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

Vorgehensweise

1. Klicken Sie auf **Menü** | **Konfiguration** | **Server-Einstellungen**, wählen Sie **Ereignisfilterung** aus, und klicken Sie dann auf **Bearbeiten**.
2. Wählen Sie die gewünschten Ereignisse aus, und klicken Sie dann auf **Speichern**.

Diese Einstellungen werden wirksam, sobald sich sämtliche Agenten beim Server gemeldet haben.

Konfigurieren automatischer Antworten

Gehen Sie wie in diesen Aufgaben beschrieben vor, um die erforderlichen Ressourcen zu konfigurieren, mit denen Sie die automatischen Antworten optimal nutzen können.

Aufgaben

- *Zuweisen von Berechtigungen für Benachrichtigungen* auf Seite 234
  Mit Berechtigungen für Benachrichtigungen können Benutzer registrierte ausführbare Dateien anzeigen, erstellen und bearbeiten.
- *Zuweisen von Berechtigungen für automatische Antworten* auf Seite 235
  Mit Berechtigungen für Antworten können Benutzer Antwortregeln für unterschiedliche Ereignistypen und Gruppen erstellen.
- *Verwalten von SNMP-Servern* auf Seite 235
  Gehen Sie wie in diesen Aufgaben beschrieben vor, um Antworten zur Verwendung Ihres SNMP-Servers (Simple Network Management Protocol) zu konfigurieren.

Zuweisen von Berechtigungen für Benachrichtigungen

Mit Berechtigungen für Benachrichtigungen können Benutzer registrierte ausführbare Dateien anzeigen, erstellen und bearbeiten.

Vorgehensweise

Definitionen zu Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

1. Klicken Sie auf **Menü** | **Benutzerverwaltung** | **Berechtigungssätze**, und erstellen Sie dann entweder einen Berechtigungssatz, oder wählen Sie einen vorhandenen Berechtigungssatz aus.
2. Klicken Sie neben **Ereignisbenachrichtigungen** auf **Bearbeiten**.
3. Wählen Sie die gewünschte Berechtigung für Benachrichtigungen aus:
   - **Keine Berechtigungen**
   - **Registrierte ausführbare Dateien anzeigen**
   - **Registrierte ausführbare Dateien erstellen und bearbeiten**
   - **Regeln und Benachrichtigungen für gesamte Systemstruktur anzeigen (setzt Zugriffsberechtigungen für Systemstrukturgruppe außer Kraft)**
4. Klicken Sie auf **Speichern**.
5. Wenn Sie einen Berechtigungssatz erstellt haben, klicken Sie auf **Menü** | **Benutzerverwaltung** | **Benutzer**.

6 Wählen Sie einen Benutzer aus, dem Sie den neuen Berechtigungssatz zuweisen möchten, und klicken Sie dann auf **Bearbeiten**.

7 Aktivieren Sie neben **Berechtigungssätze** das Kontrollkästchen für den Berechtigungssatz mit den gewünschten Berechtigungen für Benachrichtigungen, und klicken Sie dann auf **Speichern**.

Zuweisen von Berechtigungen für automatische Antworten

Mit Berechtigungen für Antworten können Benutzer Antwortregeln für unterschiedliche Ereignistypen und Gruppen erstellen.



Zum Erstellen einer Antwortregel müssen Benutzer über Berechtigungen für das Bedrohungsereignisprotokoll, Server-Tasks, entdeckte Systeme und die Systemstruktur verfügen.

Vorgehensweise

Definitionen zu Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

1. Klicken Sie auf **Menü** | **Benutzerverwaltung** | **Berechtigungssätze**, und erstellen Sie dann entweder einen Berechtigungssatz, oder wählen Sie einen vorhandenen Berechtigungssatz aus.
2. Klicken Sie neben **Automatische Antwort** auf **Bearbeiten**.
3. Wählen Sie die gewünschte Berechtigung für **Automatische Antwort** aus:
   - **Keine Berechtigungen**
   - **Antworten anzeigen; Ergebnisse zu Antworten im Server-Task-Protokoll anzeigen**
   - **Antworten erstellen, bearbeiten, anzeigen und abbrechen; Ergebnisse zu Antworten im Server-Task-Protokoll anzeigen**
4. Klicken Sie auf **Speichern**.
5. Wenn Sie einen Berechtigungssatz erstellt haben, klicken Sie auf **Menü** | **Benutzerverwaltung** | **Benutzer**.
6. Wählen Sie einen Benutzer aus, dem Sie den neuen Berechtigungssatz zuweisen möchten, und klicken Sie dann auf **Bearbeiten**.
7. Aktivieren Sie neben **Berechtigungssätze** das Kontrollkästchen für den Berechtigungssatz mit den gewünschten Berechtigungen für automatische Antworten, und klicken Sie dann auf **Speichern**.

Verwalten von SNMP-Servern

Gehen Sie wie in diesen Aufgaben beschrieben vor, um Antworten zur Verwendung Ihres SNMP-Servers (Simple Network Management Protocol) zu konfigurieren.

Sie können das Antwortsystem so konfigurieren, dass SNMP-Traps an Ihren SNMP-Server gesendet werden. Auf diese Weise können Sie SNMP-Traps an der gleichen Stelle empfangen, an der Sie Ihre Netzwerkverwaltungs-Software zum Anzeigen von detaillierten Informationen über die Systeme in Ihrer Umgebung verwenden.



Weitere Konfigurationsschritte oder das Starten eines Diensts zum Konfigurieren dieser Funktion sind nicht erforderlich.

Aufgaben

- *Bearbeiten von SNMP-Servern* auf Seite 236
  Sie können Einträge zu vorhandenen SNMP-Servern bearbeiten.
- *Löschen eines SNMP-Servers* auf Seite 237
  Sie können einen SNMP-Server im Benachrichtigungssystem löschen.
- *Importieren von MIB-Dateien* auf Seite 238
  Gehen Sie wie in dieser Aufgabe beschrieben vor, um Regeln einzurichten, nach denen Benachrichtigungen über einen SNMP-Trap an einen SNMP-Server gesendet werden.

Bearbeiten von SNMP-Servern

Sie können Einträge zu vorhandenen SNMP-Servern bearbeiten.

Definitionen zu Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

Vorgehensweise

1. Klicken Sie auf **Menü | Konfiguration | Registrierte Server**.
2. Wählen Sie in der Liste der registrierten Server den gewünschten SNMP-Server aus, und klicken Sie dann auf **Aktionen | Bearbeiten**.
3. Bearbeiten Sie nach Bedarf die folgenden Server-Einstellungen, und klicken Sie dann auf **Speichern**.

Option	Definition

Adresse	Geben Sie die Adresse des SNMP-Servers ein. Gültige Formate enthalten folgende Elemente:
	• **DNS-Name** – Gibt den DNS-Namen des Servers an. Zum Beispiel:
	`meinhost.meinefirma.com`
	• **IPv4** – Gibt die IPv4-Adresse des Servers an.
	`xxx.xxx.xxx.xxx/yy`
	• **IPv6** – Gibt die IPv6-Adresse des Servers an.
	`xxxx:xxxx:xxxx:xxxx:xxxx:xxxx/yyy`

Sicherheit	Zeigt die Sicherheitsdetails des SNMP-Servers an. • **Community** – Gibt den Community-Namen des SNMP-Protokolls an. • **SNMPv3-Sicherheit** – Gibt die SNMPv3-Sicherheitsdetails an. Dieses Feld ist nur dann aktiviert, wenn der Server die Version v3 hat. • **Sicherheitsname** – Gibt den Namen der Sicherheitseinstellungen für den SNMP-Server an. • **Authentifizierungsprotokoll** – Gibt das Protokoll an, das vom SNMP-Server zur Verifizierung der Quelle verwendet wird. • **Authentifizierungs-Passphrase** – Gibt das Kennwort für die Protokollverifizierung an. • **Authentifizierungs-Passphrase bestätigen** – Geben Sie hier das Kennwort für die Protokollverifizierung erneut ein. • **Datenschutzprotokoll** – Gibt das Protokoll an, das vom SNMP-Server zum Anpassen des vom Benutzer definierten Datenschutzes verwendet wird. Wenn Sie **AES 192** oder **AES 245** auswählen, müssen Sie die standardmäßigen Richtliniendateien durch die Version "Unlimited Strength" von der Java SE-Download-Seite von Sun ersetzen. Suchen Sie den Download **Java Cryptography Extension (JCE) Unlimited Strength Jurisdiction Policy Files 6**. Ersetzen Sie zum Anwenden der Unlimited-Strength-Richtlinien auf dem McAfee ePO-Server die JAR-Dateien der Richtlinien im Verzeichnis `EPO_VERZEICHNIS/jre/lib/security` durch die in der Datei JCE_POLICY-6.ZIP heruntergeladenen, und starten Sie den McAfee ePO-Server neu. • **Datenschutz-Passphrase** – Gibt das Kennwort für die Datenschutzprotokolleinstellungen an. • **Datenschutz-Passphrase bestätigen** – Geben Sie hier das Kennwort für die Datenschutzprotokolleinstellungen erneut ein.
SNMP-Version	Gibt die von Ihrem Server verwendete SNMP-Version an.
Test-Trap senden	Testet Ihre Konfiguration.

Löschen eines SNMP-Servers

Sie können einen SNMP-Server im Benachrichtigungssystem löschen.

Definitionen zu Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

Vorgehensweise

1. Klicken Sie auf **Menü | Konfiguration | Registrierte Server**.
2. Wählen Sie in der Liste der registrierten Server den gewünschten SNMP-Server aus, und klicken Sie dann auf **Aktionen | Löschen**.
3. Wenn Sie dazu aufgefordert werden, klicken Sie auf **Ja**.

Der SNMP-Server wird aus der Liste **Registrierte Server** entfernt.

Importieren von MIB-Dateien

Gehen Sie wie in dieser Aufgabe beschrieben vor, um Regeln einzurichten, nach denen Benachrichtigungen über einen SNMP-Trap an einen SNMP-Server gesendet werden.

Sie müssen drei MIB-Dateien aus dem Ordner `\Programme\McAfee\ePolicy Orchestrator\MIB` importieren. Die Dateien müssen in der folgenden Reihenfolge importiert werden:

1. NAI-MIB.MIB
2. TVD-MIB.MIB
3. EPO-MIB.MIB

Mithilfe dieser Dateien kann Ihr Netzwerkverwaltungsprogramm die in den SNMP-Traps enthaltenen Daten in Klartext umwandeln. Die Datei EPO-MIB.MIB ist zum Definieren der folgenden Traps von den anderen beiden Dateien abhängig:

- **epoThreatEvent** – Dieser Trap wird gesendet, wenn eine automatische Antwort für ein McAfee ePO-Bedrohungsereignis ausgelöst wird. Er enthält Variablen, die mit den Eigenschaften des Bedrohungsereignisses übereinstimmen.
- **epoStatusEvent** – Dieser Trap wird gesendet, wenn eine automatische Antwort für ein McAfee ePO-Statusereignis ausgelöst wird. Er enthält Variablen, die mit den Eigenschaften eines (Server-) Statusereignisses übereinstimmen.
- **epoClientStatusEvent** – Dieser Trap wird gesendet, wenn eine automatische Antwort für ein McAfee ePO-Client-Statusereignis ausgelöst wird. Er enthält Variablen, die mit den Eigenschaften eines Client-Statusereignisses übereinstimmen.
- **epoTestEvent** – Dies ist ein Test-Trap, der gesendet wird, wenn Sie auf den Seiten **SNMP-Server: Neu** oder **SNMP-Server: Bearbeiten** auf **Test-Trap senden** klicken.

Weitere Anweisungen zum Importieren und Implementieren von MIB-Dateien finden Sie in der Dokumentation Ihres Netzwerkverwaltungsprogramms.

Bestimmen der an den Server weiterzuleitenden Ereignisse

Mittels **Server-Einstellungen** und **Ereignisfilterung** können Sie bestimmen, welche Ereignisse an den Server weitergeleitet werden sollen.

Bevor Sie beginnen



Diese Einstellungen wirken sich darauf aus, wie viel Bandbreite in Ihrer Umgebung belegt wird und welche Ergebnisse ereignisbasierte Abfragen zurückgeben.

Vorgehensweise

Definitionen zu Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

1. Klicken Sie auf **Menü** | **Konfiguration** | **Server-Einstellungen**, wählen Sie **Ereignisfilterung** aus, und klicken Sie dann unten auf der Seite auf **Bearbeiten**. Die Seite **Ereignisfilterung: Bearbeiten** wird angezeigt.
2. Wählen Sie die Ereignisse aus, die der Agent an den Server weiterleiten soll, und klicken Sie dann auf **Speichern**.

Änderungen an diesen Einstellungen werden wirksam, nachdem alle Agenten mit dem McAfee ePO-Server kommuniziert haben.

Auswählen eines Intervalls für ePO-Benachrichtigungsereignisse

Mit dieser Einstellung wird festgelegt, wie oft **ePO-Benachrichtigungsereignisse** an das System für automatische Antworten gesendet werden.

Es gibt drei Typen von **ePO-Benachrichtigungsereignissen**:

- **Client-Ereignisse** – Das sind Ereignisse, die auf verwalteten Systemen auftreten. Zum Beispiel "Produktaktualisierung erfolgreich durchgeführt".
- **Bedrohungsreignisse** – Das sind Ereignisse, die anzeigen, dass eine potenzielle Bedrohung entdeckt wurde. Zum Beispiel "Virus entdeckt".
- **Server-Ereignisse** – Das sind Ereignisse, die auf dem Server auftreten. Zum Beispiel "Fehler bei Repository-Abruf".

Eine automatische Antwort kann nur dann ausgelöst werden, wenn das System für automatische Antworten eine Benachrichtigung erhalten hat. Es wird empfohlen, ein relativ kurzes Intervall für das Senden dieser Benachrichtigungsereignisse anzugeben. McAfee empfiehlt, ein Testintervall festzulegen, das kurz genug ist, sodass das System für automatische Antworten möglichst zeitnah auf ein Ereignis reagieren kann, jedoch nicht zu kurz, damit nicht unnötig Bandbreite belegt wird.

Vorgehensweise

Definitionen zu Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

1. Klicken Sie auf **Menü** | **Konfiguration** | **Server-Einstellungen**, wählen Sie in der Liste **Einstellungskategorien** den Eintrag **Ereignisbenachrichtigungen** aus, und klicken Sie dann auf **Bearbeiten**.
2. Geben Sie für das **Testintervall** (das standardmäßig 1 Minute beträgt) einen Wert zwischen 1 und 9.999 Minuten an, und klicken Sie dann auf **Speichern**.

Erstellen und Bearbeiten von Regeln für automatische Antworten

Gehen Sie wie in diesen Aufgaben beschrieben vor, um Regeln für automatische Antworten zu erstellen und zu bearbeiten. Auf diese Weise können Sie definieren, wann und wie eine Antwort auf ein Ereignis erfolgen soll, dass auf einem Server oder einem verwalteten System auftritt.



Regeln für automatische Antworten weisen keine abhängige Reihenfolge auf.

Aufgaben

- *Beschreiben der Regel* auf Seite 240
  Beim Erstellen einer neuen Regel können Sie eine Beschreibung hinzufügen, die Sprache festlegen, die Gruppe und den Typ des Ereignisses angeben, das die Antwort auslöst, sowie die Regel aktivieren oder deaktivieren.
- *Festlegen von Filtern für die Regel* auf Seite 240
  Sie können im Assistenten **Antwort-Generator** auf der Seite **Filter** die Filter für die Antwortregel festlegen.
- *Festlegen von Schwellenwerten für die Regel* auf Seite 241
  Sie können auf der Seite **Aggregation** des Assistenten **Antwort-Generator** festlegen, wann die Regel von dem Ereignis ausgelöst wird.
- *Konfigurieren der Aktion für Regeln zu automatischen Antworten* auf Seite 241
  Sie können die Antworten, die von der Regel ausgelöst werden, im **Antwort-Generator** auf der Seite **Antworten** konfigurieren.

Beschreiben der Regel

Beim Erstellen einer neuen Regel können Sie eine Beschreibung hinzufügen, die Sprache festlegen, die Gruppe und den Typ des Ereignisses angeben, das die Antwort auslöst, sowie die Regel aktivieren oder deaktivieren.

Definitionen zu Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

Vorgehensweise

1. Klicken Sie auf **Menü** | **Automatisierung** | **Automatische Antworten**, und klicken Sie dann auf **Aktionen** | **Neue Antwort** oder neben einer Regel auf **Bearbeiten**.
2. Geben Sie auf der Seite **Beschreibung** einen eindeutigen Namen und mögliche Anmerkungen zu der Regel ein.

   Regelnamen müssen auf einem Server eindeutig sein. Wenn zum Beispiel ein Benutzer eine Regel namens "Notfallbenachrichtigung" erstellt, darf kein anderer Benutzer (einschließlich Administratoren) eine Regel mit dem gleichen Namen erstellen.
3. Wählen Sie im Menü **Sprache** die Sprache für die Regel aus.
4. Wählen Sie die **Ereignisgruppe** und den **Ereignistyp** aus, von denen die Antwort ausgelöst wird.
5. Wählen Sie neben **Status** aus, ob die Regel **Aktiviert** oder **Deaktiviert** ist.
6. Klicken Sie auf **Weiter**.

Festlegen von Filtern für die Regel

Sie können im Assistenten **Antwort-Generator** auf der Seite **Filter** die Filter für die Antwortregel festlegen.

Definitionen zu Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

Vorgehensweise

1. Wählen Sie in der Liste **Verfügbare Eigenschaften** die gewünschte Eigenschaft aus, und geben Sie den Wert an, nach dem das Ergebnis der Antwort gefiltert werden soll.

   Welche Eigenschaften zur Verfügung stehen, richtet sich danach, welcher Ereignistyp und welche Ereignisgruppe auf der Seite **Beschreibung** des Assistenten ausgewählt sind.
2. Klicken Sie auf **Weiter**.

Festlegen von Schwellenwerten für die Regel

Sie können auf der Seite **Aggregation** des Assistenten **Antwort-Generator** festlegen, wann die Regel von dem Ereignis ausgelöst wird.

Schwellenwerte von Regeln sind eine Kombination von Aggregation, Beschränkung und Gruppierung.

Definitionen zu Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

Vorgehensweise

1. Aktivieren Sie neben **Aggregation** die Option **Diese Antwort für jedes Ereignis auslösen**, oder wählen Sie die Option **Diese Antwort auslösen beim Auftreten mehrerer Ereignisse in** aus, und legen Sie einen entsprechenden Zeitraum fest. In letzterem Fall geben Sie den Zeitraum in Minuten, Stunden oder Tagen an.
2. Wenn Sie die Option **Diese Antwort auslösen beim Auftreten mehrerer Ereignisse in** ausgewählt haben, können Sie festlegen, dass eine Antwort ausgelöst werden soll, wenn die angegebenen Bedingungen erfüllt sind. Diese Bedingungen sind eine beliebige Kombination der folgenden beiden Punkte:
   - **Die Anzahl eindeutiger Werte für eine Ereigniseigenschaft erreicht einen Mindestwert.** Diese Bedingung wird verwendet, wenn ein bestimmter Wert für das Auftreten der Ereigniseigenschaft ausgewählt ist.
   - **Wenn mindestens die folgende Anzahl von Ereignissen aufgetreten ist.** Geben Sie eine bestimmte Anzahl von Ereignissen ein.

   Sie können eine oder beide Optionen auswählen. So können Sie die Regel zum Beispiel so festlegen, dass diese Antwort ausgelöst werden soll, wenn die ausgewählte Ereigniseigenschaft mehr als 300 Mal auftritt, oder wenn die Anzahl der Ereignisse den Wert 3.000 überschreitet, je nachdem, welcher Schwellenwert zuerst überschritten wird.
3. Wählen Sie neben **Gruppierung** aus, ob die aggregierten Ereignisse gruppiert werden sollen. Wenn Sie festlegen, dass die aggregierten Ereignisse gruppiert werden sollen, müssen Sie angeben, nach welcher Eigenschaft des Ereignisses die Gruppierung erfolgen soll.
4. Aktivieren Sie neben **Beschränkung** gegebenenfalls die Option **Diese Antwort nicht häufiger auslösen als alle**, und legen Sie einen Zeitraum fest, nach dessen Verstreichen die Regel wieder Benachrichtigungen senden darf.

   Der Zeitraum kann in Minuten, Stunden oder Tagen angegeben werden.
5. Klicken Sie auf **Weiter**.

Konfigurieren der Aktion für Regeln zu automatischen Antworten

Sie können die Antworten, die von der Regel ausgelöst werden, im **Antwort-Generator** auf der Seite **Antworten** konfigurieren.

Mithilfe der Schaltflächen **+** und - neben der Dropdown-Liste für den Benachrichtigungstyp können Sie die Regel so konfigurieren, dass sie mehrere Aktionen auslöst.

Vorgehensweise

Definitionen zu Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

1. Wenn die Benachrichtigung in Form einer E-Mail- oder Text-Pager-Nachricht gesendet werden soll, wählen Sie in der Dropdown-Liste **E-Mail senden** aus.
   - a Klicken Sie neben **Empfänger** auf die Schaltfläche zum Durchsuchen […], und wählen Sie die Empfänger für die Nachricht aus. Diese Liste der verfügbaren Empfänger stammt aus den Kontakten (**Menü** | **Benutzerverwaltung** | **Kontakte**). Alternativ dazu können Sie die E-Mail-Adressen auch manuell eingeben, getrennt durch ein Komma.
   - b Wählen Sie die Wichtigkeit der Benachrichtigungs-E-Mail aus.
   - c Geben Sie den **Betreff** für die Nachricht ein. Optional können Sie auch jede verfügbare Variable direkt in die Betreffzeile eingeben.
   - d Geben Sie den Text ein, der im **Nachrichtentext** der Nachricht angezeigt werden soll. Optional können Sie auch jede verfügbare Variable direkt in den Textteil eingeben.
   - e Klicken Sie abschließend auf **Weiter** oder auf **+**, um eine weitere Benachrichtigung hinzuzufügen.
2. Wenn die Benachrichtigung in Form eines SNMP-Traps gesendet werden soll, wählen Sie in der Dropdown-Liste **SNMP-Trap senden** aus.
   - a Wählen Sie in der Dropdown-Liste den gewünschten SNMP-Server aus.
   - b Wählen Sie den Typ des Werts aus, der in dem SNMP-Trap gesendet werden soll.
     - **Wert**
     - **Anzahl eindeutiger Werte**
     - **Liste eindeutiger Werte**
     - **Liste aller Werte**

     Nicht alle Ereignisse beinhalten diese Informationen. Wenn zu einigen der von Ihnen ausgewählten Optionen nichts angezeigt wird, dann steht diese Information in der Ereignisdatei nicht zur Verfügung.
   - c Klicken Sie abschließend auf **Weiter** oder auf **+**, um eine weitere Benachrichtigung hinzuzufügen.
3. Wenn Sie möchten, dass die Benachrichtigung einen externen Befehl ausführt, wählen Sie in der Dropdown-Liste **Externen Befehl ausführen** aus.
   - a Wählen Sie die gewünschten Dateien unter **Registrierte ausführbare Dateien** aus, und geben Sie etwaige **Argumente** für den Befehl ein.
   - b Klicken Sie abschließend auf **Weiter** oder auf **+**, um eine weitere Benachrichtigung hinzuzufügen.
4. Wenn Sie möchten, dass die Benachrichtigung ein Problem erstellt, wählen Sie in der Dropdown-Liste **Problem erstellen** aus.
   - a Wählen Sie den Typ des zu erstellenden Problems aus.
   - b Geben Sie einen eindeutigen Namen und eventuelle Anmerkungen zu dem Problem ein. Optional können Sie auch jede der verfügbaren Variablen direkt in den Namen und die Beschreibung einfügen.
   - c Wählen Sie in den entsprechend Dropdown-Listen den **Zustand**, die **Priorität**, den **Schweregrad** und die **Lösung** für das Problem aus.

   d Geben Sie den Namen des Beauftragten in das Textfeld ein.

   e Klicken Sie abschließend auf **Weiter** oder auf **+**, um eine weitere Benachrichtigung hinzuzufügen.

5. Wenn Sie möchten, dass die Benachrichtigung einen geplanten Task ausführt, wählen Sie in der Dropdown-Liste **Server-Task ausführen** aus.

   a Wählen Sie in der Dropdown-Liste **Auszuführender Task** den Task aus, der ausgeführt werden soll.

   b Klicken Sie abschließend auf **Weiter** oder auf **+**, um eine weitere Benachrichtigung hinzuzufügen.

6. Überprüfen Sie die Informationen auf der Seite **Zusammenfassung**, und klicken Sie dann auf **Speichern**.

Die neue Antwortregel wird in der Liste **Antworten** angezeigt.

17 McAfee Labs-Sicherheitsbedrohungen

McAfee Labs stellt aktuelle Informationen zu Sicherheitsbedrohungen bereit, die Ihr Netzwerk möglicherweise gefährden können.

Inhalt

McAfee Labs-Informationen zu Bedrohungen

Auf der Seite **McAfee Labs-Sicherheitsbedrohungen** werden Sie über die zehn wichtigsten Bedrohungen mit mittlerem bis hohem Risiko für geschäftliche Benutzer informiert. Nun müssen Sie nicht mehr manuell nach diesen Informationen in der Presse (TV, Radio bzw. Zeitungen), auf internationalen Websites, Mailing-Listen oder bei anderen Quellen suchen. Sie werden von McAfee Labs automatisch über diese Bedrohungen benachrichtigt.

Schutzstatus und Risikobewertung

Sie können auf einfache Weise erkennen, ob die neuen DAT- und Scan-Modul-Dateien im Zweig **Aktuell** des Master-Repositorys ausreichend Schutz vor den zehn wichtigsten Bedrohungen bieten. Wenn dies nicht der Fall ist, können Sie den höchsten Risikograd neuer Bedrohungen bestimmen.

Schutz verfügbar

Die DAT- und Scan-Modul-Dateien im Repository bieten bereits Schutz vor allen McAfee Labs bekannten Bedrohungen. Um festzustellen, ob alle verwalteten Systeme geschützt sind, fragen Sie die Abdeckung der DAT- und Scan-Modul-Dateien ab.

Schutz für Bedrohungen mit mittlerem bis niedrigem Risiko steht aus

Die aktualisierte DAT-Datei für Bedrohungen, die von McAfee Labs als mittleres Risiko eingestuft wurden, steht noch aus. Es ist jedoch ein aktualisierter Schutz in Form einer ergänzenden Virusdefinitionsdatei (EXTRA.DAT) verfügbar. Sie können diese Datei manuell herunterladen, wenn Sie Schutz benötigen, bevor die nächste DAT-Datei verfügbar ist (z. B. bei einem Virenausbruch).

Schutz für Bedrohungen mit hohem Risiko steht aus

Die aktualisierte DAT-Datei für Bedrohungen, die von McAfee Labs als hohes Risiko eingestuft wurden, steht noch aus. Es ist jedoch ein aktualisierter Schutz in Form einer ergänzenden Virusdefinitionsdatei (EXTRA.DAT) verfügbar. Sie können diese Datei manuell herunterladen, wenn Sie Schutz benötigen, bevor die nächste DAT-Datei verfügbar ist (z. B. bei einem Virenausbruch).

Arbeiten mit McAfee Labs-Sicherheitsbedrohungen

Gehen Sie wie in diesen Aufgaben beschrieben vor, um Benachrichtigungen über Bedrohungen als gelesen oder ungelesen zu kennzeichnen oder sie zu löschen. Die Daten werden nach dem Datum sortiert, an dem die Bedrohung entdeckt wurde. Darüber hinaus können Sie auf den Namen einer Bedrohung klicken, um auf der McAfee Labs-Website Informationen zur jeweiligen Bedrohung anzuzeigen.



Für jedes Benutzerkonto wird eine eigene Seite **McAfee Labs-Sicherheitsbedrohungen** angezeigt. Wenn Benachrichtigungen über Bedrohungen von einem Benutzer gelöscht oder als gelesen bzw. ungelesen gekennzeichnet werden, hat dies keine Auswirkungen darauf, wie diese Benachrichtigungen für andere Benutzer angezeigt werden, die sich anmelden.

Aufgaben

- *Konfigurieren des Aktualisierungsintervalls für McAfee Labs-Sicherheitsbedrohungen* auf Seite 246
  Das Aktualisierungsintervall für McAfee Labs-Sicherheitsbedrohungen können Sie mithilfe der **Server-Einstellungen** konfigurieren.
- *Anzeigen von Benachrichtigungen über Bedrohungen* auf Seite 246
  Sie können Benachrichtigungen über Bedrohungen anzeigen, diese als gelesen oder ungelesen markieren, Bedrohungen nach deren Wichtigkeit filtern oder danach, ob sie gelesen oder nicht gelesen wurden.
- *Löschen von Benachrichtigungen über Bedrohungen* auf Seite 247
  Gehen Sie wie in dieser Aufgabe beschrieben vor, um Benachrichtigungen über Bedrohungen auf der Seite **McAfee Labs-Sicherheitsbedrohungen** zu löschen. Benachrichtigungen über Bedrohungen, für die der Schutz noch aussteht, können Sie nicht löschen.

Konfigurieren des Aktualisierungsintervalls für McAfee Labs-Sicherheitsbedrohungen

Das Aktualisierungsintervall für McAfee Labs-Sicherheitsbedrohungen können Sie mithilfe der **Server-Einstellungen** konfigurieren.

Vorgehensweise

Definitionen zu Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

1. Klicken Sie auf **Menü** | **Konfiguration** | **Server-Einstellungen**, wählen Sie **McAfee Labs-Sicherheitsbedrohungen** aus, und klicken Sie dann auf **Bearbeiten**.
2. Wählen Sie bei **Aktualisierung** eine der folgenden Optionen aus:
   - **McAfee Labs-Sicherheitsbedrohungen aktualisieren alle** – Legen Sie fest, wann die Aktualisierungen stattfinden sollen. Geben Sie dazu eine Zahl ein, und wählen Sie eine Zeiteinheit in der Liste aus.
   - **McAfee Labs-Sicherheitsbedrohungen nicht aktualisieren** – Aktivieren Sie diese Option, um Aktualisierungen zu beenden.
3. Klicken Sie auf **Speichern**.

Anzeigen von Benachrichtigungen über Bedrohungen

Sie können Benachrichtigungen über Bedrohungen anzeigen, diese als gelesen oder ungelesen markieren, Bedrohungen nach deren Wichtigkeit filtern oder danach, ob sie gelesen oder nicht gelesen wurden.

Vorgehensweise

Definitionen zu Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

1. Klicken Sie auf **Menü | Berichterstellung | McAfee Labs**.
2. Wenn Sie die anzeigbaren Benachrichtigungen eingrenzen möchten, wählen Sie in der Dropdown-Liste **Voreingestellt** eine Option aus.
3. Wenn Sie Benachrichtigungen als gelesen oder ungelesen kennzeichnen möchten, wählen Sie die gewünschten Bedrohungen aus, und klicken Sie dann nach Bedarf auf **Aktionen | Als gelesen markieren** oder **Als ungelesen markieren**. Unter Umständen müssen Sie in der Dropdown-Liste **Voreingestellt** die Option **Gelesen** oder **Ungelesen** auswählen, um die zu kennzeichnenden Benachrichtigungen anzuzeigen.

Löschen von Benachrichtigungen über Bedrohungen

Gehen Sie wie in dieser Aufgabe beschrieben vor, um Benachrichtigungen über Bedrohungen auf der Seite **McAfee Labs-Sicherheitsbedrohungen** zu löschen. Benachrichtigungen über Bedrohungen, für die der Schutz noch aussteht, können Sie nicht löschen.

Vorgehensweise

Definitionen zu Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

1. Klicken Sie auf **Menü | Berichterstellung | McAfee Labs**.
2. Wählen Sie Benachrichtigungen über Bedrohungen aus, für die bereits Schutz verfügbar ist, klicken Sie dann auf **Aktionen**, und wählen Sie **Löschen** aus.

Überwachung und Berichterstellung zum Netzwerk-Sicherheitsstatus

Mithilfe anpassbarer Dashboards können Sie wichtige Sicherheitszustände auf einen Blick überwachen und diesen Status in vorkonfigurierten, anpassbaren Abfragen und Berichten an relevante Mitarbeiter und Entscheidungsträger melden.

18 Dashboards

Das konstante Überwachen Ihrer Umgebung ist schwierig. Dashboards helfen Ihnen dabei.

Dashboards sind Sammlungen von Monitoren. Diese Monitore können sehr unterschiedlich sein, d. h. diagrammbasierte Abfragen ebenso wie kleine Web-Anwendungen, z. B. McAfee Labs-Sicherheitsbedrohungen.

Das Verhalten und Aussehen eines Monitors wird einzeln konfiguriert.

Die Benutzer müssen über die entsprechenden Berechtigungen verfügen, um Dashboards verwenden, erstellen, bearbeiten und löschen zu können.

Inhalt

Erstmaliges Konfigurieren von Dashboards

Die nachfolgenden allgemeinen Schritte beschreiben die Vorgehensweise bei der erstmaligen Konfiguration von Dashboards.

1. Der ePolicy Orchestrator-Server verfügt über ein Standard-Dashboard, das angezeigt wird, wenn Sie zum ersten Mal ein Dashboard laden.
2. Erstellen Sie alle benötigten Dashboards und deren Monitore.
3. Wenn Sie ePolicy Orchestrator das nächste Mal starten, wird das zuletzt verwendete Dashboard geladen.

Arbeiten mit Dashboards

Dashboards können u. a. erstellt, geändert, dupliziert und exportiert werden, sodass Sie Ihre Umgebung auf einem Blick überwachen können.

Gehen Sie wie in diesen Aufgaben beschrieben vor, wenn Sie mit Dashboards arbeiten.



Die im Lieferumfang von ePolicy Orchestrator enthaltenen Standard-Dashboards und vordefinierten Abfragen können nicht geändert oder gelöscht werden. Wenn Sie eines dieser Dashboards oder eine dieser Abfragen ändern möchten, müssen Sie es bzw. sie duplizieren und umbenennen. Anschließend können Sie das umbenannte Duplikat ändern.

Aufgaben

- *Verwalten von Dashboards* auf Seite 252
  Sie können Berechtigungen für Dashboards erstellen, bearbeiten, duplizieren, löschen und diese Berechtigungen zu Dashboards zuweisen.
- *Exportieren und Importieren von Dashboards* auf Seite 254
  Nachdem Sie Ihre Dashboards und Monitore fertig definiert haben, können diese am schnellsten auf andere McAfee ePO-Server migriert werden, indem Sie sie exportieren und auf den anderen Servern importieren.

Verwalten von Dashboards

Sie können Berechtigungen für Dashboards erstellen, bearbeiten, duplizieren, löschen und diese Berechtigungen zu Dashboards zuweisen.

> **Bevor Sie beginnen**
>
> Zum Ändern eines Dashboards müssen Sie über Schreibberechtigungen verfügen.

Vorgehensweise

Definitionen zu Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

1. Klicken Sie auf **Menü** | **Berichterstellung** | **Dashboards**, um zur Seite **Dashboards** zu gelangen.
2. Wählen Sie eine der folgenden Aktionen aus.

<table>
<tr><th>Aktion</th><th>Vorgehensweise</th></tr>
<tr><td>Erstellen von Dashboards</td><td>Zum Erstellen einer anderen Ansicht Ihrer Umgebung erstellen Sie ein neues Dashboard.
1 Klicken Sie auf Dashboard-Aktionen | Neu.
Das Dialogfeld Neues Dashboard wird angezeigt.
2 Geben Sie einen Namen für das Dashboard ein, wählen Sie eine Option für die Dashboard-Sichtbarkeit aus, und klicken Sie auf OK.
Ein neues leeres Dashboard wird angezeigt. Dem neuen Dashboard können je nach Bedarf Monitore hinzugefügt werden.</td></tr>
<tr><td>Bearbeiten und Zuweisen von Dashboard-Berichtigungen</td><td>Dashboards werden nur Benutzern mit entsprechender Berechtigung angezeigt. Die Dashboards zugewiesenen Berechtigungen sind mit denen von Abfragen oder Berichten identisch. Die Dashboards sind entweder ganz privat, ganz öffentlich oder mit einem oder mehreren Berechtigungssätzen freigegeben.
1 Klicken Sie auf Dashboard-Aktionen | Bearbeiten.
Das Dialogfeld Dashboard bearbeiten wird angezeigt.
2 Wählen Sie eine Berechtigung aus:
• Dieses Dashboard nicht freigeben
• Dieses Dashboard für alle freigeben
• Dieses Dashboard für die folgenden Berechtigungssätze freigeben
Bei dieser Option müssen Sie außerdem mindestens einen Berechtigungssatz auswählen.
3 Klicken Sie auf OK, um das Dashboard zu ändern.
Sie können auch ein Dashboard erstellen, das umfangreichere Berechtigungen als eine oder mehrere im Dashboard enthaltene Abfragen besitzt. In solchen Fällen wird Benutzern, die über Zugriff auf die zugrundeliegenden Daten verfügen, beim Öffnen des Dashboards die Abfrage angezeigt. Benutzern ohne Zugriff auf die zugrundeliegenden Daten wird eine Meldung mit dem Inhalt angezeigt, dass sie nicht über die erforderlichen Berechtigungen für diese Abfrage verfügen. Wenn die Abfrage als privat für den Dashboard-Ersteller festgelegt ist, kann sie nur vom Ersteller geändert oder aus dem Dashboard entfernt werden.</td></tr>
</table>

<table>
<tr><th>Aktion</th><th>Vorgehensweise</th></tr>
<tr><td>Duplizieren von Dashboards</td><td>Manchmal lässt sich ein neues Dashboard am einfachsten erstellen, indem ein vorhandenes Dashboard, das dem gewünschten Ergebnis am nächsten kommt, kopiert wird.
1 Klicken Sie auf Dashboard-Aktionen | Duplizieren.
Das Dialogfeld Dashboard duplizieren wird angezeigt.
2 ePolicy Orchestrator erstellt einen Namen für die Kopie, indem an den Namen des Originals der Hinweis (Kopie) angehängt wird. Wenn Sie diesen Namen ändern möchten, geben Sie den von Ihnen gewünschten Namen ein, und klicken Sie dann auf OK.
Das duplizierte Dashboard wird nun geöffnet.
Das Duplikat ist eine exakte Kopie des Original-Dashboards einschließlich aller Berechtigungen. Nur der Name ist anders.</td></tr>
<tr><td>Löschen von Dashboards</td><td>1 Klicken Sie auf Dashboard-Aktionen | Löschen.
Das Dialogfeld Dashboard löschen wird angezeigt.
2 Klicken Sie auf OK, um das Dashboard zu löschen.
Das Dashboard wurde gelöscht, und es wird das Standard-Dashboard des Systems angezeigt. Benutzern, denen das gelöschte Dashboard vor dem Abmelden als letztes Dashboard angezeigt wurde, wird bei ihrer nächsten Anmeldung das Standard-Dashboard des Systems angezeigt.</td></tr>
</table>

Exportieren und Importieren von Dashboards

Nachdem Sie Ihre Dashboards und Monitore fertig definiert haben, können diese am schnellsten auf andere McAfee ePO-Server migriert werden, indem Sie sie exportieren und auf den anderen Servern importieren.

Bevor Sie beginnen

Für den Import eines Dashboards müssen Sie Zugriff auf ein zuvor exportiertes, in einer XML-Datei enthaltenes Dashboard haben.

Ein als XML-Datei exportiertes Dashboard kann in dasselbe oder ein anderes System importiert werden.

Vorgehensweise

Definitionen zu Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

1 Klicken Sie auf **Menü | Berichterstellung | Dashboards**.

2 Wählen Sie eine der folgenden Aktionen aus.

Aktion	Vorgehensweise
Exportieren von Dashboards	1 Klicken Sie auf **Dashboard-Aktionen | Exportieren**. Ihr Browser versucht, gemäß den Browser-Einstellungen eine XML-Datei herunterzuladen. 2 Speichern Sie die exportierte XML-Datei in einem geeigneten Speicherort.
Importieren von Dashboards	1 Klicken Sie auf **Dashboard-Aktionen | Importieren**. Das Dialogfeld **Dashboard importieren** wird angezeigt. 2 Klicken Sie auf **Durchsuchen**, und wählen Sie die XML-Datei aus, die ein exportiertes Dashboard enthält. Klicken Sie auf **Öffnen**. 3 Klicken Sie auf **Speichern**. Das Bestätigungsdialogfeld **Dashboard importieren** wird angezeigt. Der Name des Dashboards in der Datei sowie der Name, den es im System haben wird, werden angezeigt. Standardmäßig ist dies der Name, unter dem das Dashboard exportiert wurde, an den der Zusatz "(importiert)" angehängt ist. 4 Klicken Sie auf **OK**. Wenn Sie das Dashboard nicht importieren möchten, klicken Sie auf **Schließen**. Das importierte Dashboard wird angezeigt. Unabhängig von den Berechtigungen zum Zeitpunkt des Exports werden importierten Dashboards eigene Berechtigungen zugewiesen. Nach dem Import müssen Sie die Berechtigungen explizit festlegen.

Arbeiten mit Dashboard-Monitoren

Sie können Dashboard-Monitore anpassen und ändern.

Gehen Sie wie in diesen Aufgaben beschrieben vor, wenn Sie mit Dashboard-Monitoren arbeiten.

Aufgaben

- *Verwalten von Dashboard-Monitoren* auf Seite 255
  Sie können Monitore für Dashboards erstellen, zu Dashboards hinzufügen und aus diesen entfernen.
- *Verschieben und Ändern der Größe von Dashboard-Monitoren* auf Seite 256
  Monitore können so verschoben und in der Größe angepasst werden, dass der Platz auf dem Bildschirm effizient genutzt wird.

Verwalten von Dashboard-Monitoren

Sie können Monitore für Dashboards erstellen, zu Dashboards hinzufügen und aus diesen entfernen.

Bevor Sie beginnen

Sie benötigen Schreibberechtigungen für das Dashboard, das Sie ändern möchten.

Vorgehensweise

Definitionen zu Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

1 Klicken Sie auf **Menü | Berichterstellung | Dashboards**. Wählen Sie in der Dropdown-Liste **Dashboard** ein Dashboard aus.

2 Wählen Sie eine der folgenden Aktionen aus.

<table>
<tr><th>Aktion</th><th>Vorgehensweise</th></tr>
<tr><td>Hinzufügen eines Monitors</td><td>1 Klicken Sie auf Monitor hinzufügen.
Die Monitorgalerie wird oben auf dem Bildschirm angezeigt.
2 Wählen Sie in der Dropdown-Liste Anzeigen eine Monitorkategorie aus.
Die in dieser Kategorie verfügbaren Monitore werden in der Galerie angezeigt.
3 Ziehen Sie einen Monitor auf das Dashboard. Wenn Sie den Cursor im Dashboard bewegen, wird die jeweils nächstgelegene zulässige Position hervorgehoben, an der der Monitor abgelegt werden kann. Legen Sie den Monitor an der gewünschten Position ab.
Das Dialogfeld Neuer Monitor wird angezeigt.
4 Konfigurieren Sie den Monitor gemäß Ihren Anforderungen (jeder Monitor hat seine eigenen Konfigurationsoptionen), und klicken Sie dann auf OK.
5 Wenn Sie die Monitore zum Dashboard hinzugefügt haben, klicken Sie auf Speichern, um das neu konfigurierte Dashboard zu speichern.
6 Klicken Sie nach Abschluss Ihrer Änderungen auf Schließen.
Wenn Sie zu einem Dashboard einen Monitor vom Typ Anzeige für benutzerdefinierte URLs hinzufügen, der Adobe Flash-Inhalte oder ActiveX-Steuerelemente enthält, können diese Inhalte möglicherweise Menüs von ePolicy Orchestrator verdecken, sodass auf Teile des Menüs nicht mehr zugegriffen werden kann.</td></tr>
<tr><td>Bearbeiten eines Monitors</td><td>Von jedem Monitortyp werden andere Konfigurationsoptionen unterstützt. Bei einem Abfrage-Monitor wären das zum Beispiel Änderungen bei der Abfrage, der Datenbank und dem Aktualisierungsintervall.
1 Wählen Sie einen Monitor aus, den Sie verwalten möchten, klicken Sie auf den Pfeil in seiner oberen linken Ecke, und wählen Sie Monitor bearbeiten aus.
Das Dialogfeld für die Konfiguration des Monitors wird angezeigt.
2 Wenn Sie die gewünschten Änderungen an den Einstellungen des Monitors vorgenommen haben, klicken Sie auf OK. Wenn Sie keine Änderungen vornehmen möchten, klicken Sie auf Abbrechen.
3 Wenn Sie die damit verbundenen Änderungen am Dashboard speichern möchten, klicken Sie auf Speichern. Andernfalls klicken Sie auf Verwerfen.</td></tr>
<tr><td>Entfernen eines Monitors</td><td>1 Wählen Sie einen Monitor aus, den Sie entfernen möchten, klicken Sie auf den Pfeil in seiner oberen linken Ecke, und wählen Sie Monitor entfernen aus.
Das Dialogfeld für die Konfiguration des Monitors wird angezeigt.
2 Wenn Sie die Änderungen am Dashboard vorgenommen haben, klicken Sie auf Speichern. Klicken Sie auf Verwerfen, wenn Sie das Dashboard auf seine vorherigen Einstellungen zurücksetzen möchten.</td></tr>
</table>

Verschieben und Ändern der Größe von Dashboard-Monitoren

Monitore können so verschoben und in der Größe angepasst werden, dass der Platz auf dem Bildschirm effizient genutzt wird.

Bevor Sie beginnen

Sie benötigen Schreibberechtigungen für das Dashboard, das Sie ändern möchten.

Sie können bei vielen Dashboard-Monitoren die Größe ändern. Wenn rechts unten im Monitor kleine diagonale Linien angezeigt werden, können Sie dessen Größe ändern. Monitore werden mittels Ziehen und Ablegen innerhalb des aktuellen Dashboards verschoben und in der Größe verändert.

Vorgehensweise

Definitionen zu Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

1. Verschieben Sie einen Monitor, oder ändern Sie dessen Größe.
   - So verschieben Sie einen Dashboard-Monitor
     1. Ziehen Sie den Monitor an seiner Titelleiste an die gewünschte Position.

        Wenn Sie den Cursor bewegen, wird der Umriss des Monitors an die nächste für ihn verfügbare Position verschoben.
     2. Wenn sich der Umriss an der gewünschten Position befindet, legen Sie den Monitor dort ab.

        Wenn Sie versuchen, den Monitor an einer unzulässigen Stelle abzulegen, kehrt er an seine vorherige Position zurück.
   - So ändern Sie die Größe eines Dashboard-Monitors
     1. Ziehen Sie das Symbol für die Größenänderung in der rechten unteren Ecke des Monitors zu einer geeigneten Position.

        Während Sie den Cursor bewegen, ändert der Umriss des Monitors seine Form und zeigt die in der jeweiligen Cursor-Position unterstützte Größe an. Für Monitore kann es Beschränkungen hinsichtlich der minimalen oder maximalen Größe geben.
     2. Wenn der Umriss die gewünschte Größe aufweist, lassen Sie die Maustaste los.

        Wenn Sie den Monitor auf eine Größe einstellen möchten, die an der derzeitigen Position des Monitors nicht möglich ist, wird die vorherige Größe wiederhergestellt.
2. Klicken Sie auf **Speichern**. Wenn Sie die vorherige Konfiguration wiederherstellen möchten, klicken Sie auf **Verwerfen**.

Standard-Dashboards und deren Monitore

Diese Version von ePolicy Orchestrator enthält verschiedene Standard-Dashboards, von denen jedes über eigene Standard-Monitore verfügt.



Alle anderen Dashboards außer dem Standard-Dashboard (meist **McAfee ePO-Zusammenfassung**) befinden sich im Besitz des Administrators, von dem ePolicy Orchestrator installiert wurde. Der Administrator, der die Installation durchgeführt hat, muss die Berechtigungen auf zusätzlichen Dashboards ändern, bevor andere McAfee ePO-Benutzer sie anzeigen können.

Das Dashboard "Audit"

Das Dashboard **Audit** gibt einen Überblick über Aktivitäten auf einem McAfee ePO-Server, die mit Zugriffen in Verbindung stehen. Dieses Dashboard verfügt über die folgenden Monitore:

- **Fehlgeschlagene Anmeldeversuche in den letzten 30 Tagen** – Zeigt eine nach Benutzer gruppierte Liste aller fehlgeschlagenen Anmeldeversuche in den letzten 30 Tagen an.
- **Erfolgreiche Anmeldeversuche in den letzten 30 Tagen** – Zeigt eine nach Benutzer gruppierte Liste aller erfolgreichen Anmeldeversuche in den letzten 30 Tagen an.
- **Änderungsverlauf von Richtlinienzuweisungen nach Benutzer** – Zeigt einen nach Benutzer gruppierten Bericht an, der alle Richtlinienzuweisungen aus den letzten 30 Tagen laut dem Audit-Protokoll enthält.

- **Konfigurationsänderungen nach Benutzer** – Zeigt einen nach Benutzer gruppierten Bericht an, der alle als sensibel geltenden Aktionen der letzten 30 Tage aus dem Audit-Protokoll enthält.
- **Server-Konfigurationen nach Benutzer** – Zeigt einen nach Benutzer gruppierten Bericht an, der Server-Konfigurationsaktionen der letzten 30 Tage aus dem Audit-Protokoll enthält.
- **Schnelle Systemsuche** – Sie können nach Systemen anhand des Systemnamens, der IP-Adresse, der MAC-Adresse, dem Benutzernamen oder der Agenten-GUID suchen.

Das Dashboard "McAfee ePO-Zusammenfassung"

Das Dashboard **McAfee ePO-Zusammenfassung** besteht aus einem Satz von Monitoren, die zusammengefasste Informationen und Links zu weiteren Informationen von McAfee enthalten. Dieses Dashboard verfügt über die folgenden Monitore:

- **McAfee Labs-Bedrohungshinweise** – Zeigt den verfügbaren Schutz, neue gemeldete Bedrohungen, aktuell verfügbare Versionen von DAT- und Scan-Modul-Dateien und (sofern unter **Eigenes Repository** vorhanden) einen Link zur Seite **McAfee Labs-Sicherheitsbedrohungen** sowie den Zeitpunkt der letzten Überprüfung an.
- **Systeme pro Gruppe der obersten Ebene** – Zeigt ein Balkendiagramm Ihrer verwalteten Systeme an, organisiert nach der obersten Systemstrukturgruppe.
- **Schnelle Systemsuche** – Sie können nach Systemen anhand des Systemnamens, der IP-Adresse, der MAC-Adresse, dem Benutzernamen oder der Agenten-GUID suchen.
- **McAfee-Links** – Zeigt unter anderem Links zum technischen Support von McAfee, zu Escalation-Tools und zur Vireninformationsbibliothek an.
- **Compliance-Übersicht von McAfee Agent und VirusScan Enterprise (für Windows)** – Zeigt in einem booleschen Kreisdiagramm an, welche verwalteten Systeme in Ihrer Umgebung mit der Version von VirusScan Enterprise (für Windows), McAfee Agent und den DAT-Dateien konform bzw. nicht konform sind.
- **Malware-Entdeckungsverlauf** – Zeigt ein Liniendiagramm mit der Anzahl der internen Virenentdeckungen innerhalb des letzten Quartals an.

Das Dashboard "Management"

Das **Management**-Dashboard verfügt über einen Satz von Monitoren, die zusammengefasste Berichte über Sicherheitsbedrohungen und Compliance geben und Links zu spezielleren Produktinformationen und McAfee-spezifischen Informationen enthalten. Dieses Dashboard verfügt über die folgenden Monitore:

- **McAfee Labs-Bedrohungshinweise** – Zeigt den verfügbaren Schutz, neue gemeldete Bedrohungen, aktuell verfügbare Versionen von DAT- und Scan-Modul-Dateien und (sofern unter **Eigenes Repository** vorhanden) einen Link zur Seite **McAfee Labs-Sicherheitsbedrohungen** sowie den Zeitpunkt der letzten Überprüfung an.
- **Malware-Entdeckungsverlauf** – Zeigt ein Liniendiagramm mit der Anzahl der internen Virenentdeckungen innerhalb des letzten Quartals an.
- **Produktausbringungen in den letzten 24 Stunden** – Zeigt ein boolesches Kreisdiagramm aller Produktausbringungen der letzten 24 Stunden an. Erfolgreiche Ausbringungen werden grün dargestellt.
- **Produktaktualisierungen in den letzten 24 Stunden** – Zeigt ein boolesches Kreisdiagramm aller Produktaktualisierungen der letzten 24 Stunden an. Erfolgreiche Aktualisierungen werden grün dargestellt.

Das Dashboard "Produktausbringung"

Das Dashboard **Produktausbringung** gibt einen Überblick über Aktivitäten im Netzwerk bezüglich der Ausbringung und Aktualisierung von Produkten. Dieses Dashboard verfügt über die folgenden Monitore:

- **Produktausbringungen in den letzten 24 Stunden** – Zeigt ein boolesches Kreisdiagramm aller Produktausbringungen der letzten 24 Stunden an. Erfolgreiche Ausbringungen werden grün dargestellt.
- **Produktaktualisierungen in den letzten 24 Stunden** – Zeigt ein boolesches Kreisdiagramm aller Produktaktualisierungen der letzten 24 Stunden an. Erfolgreiche Aktualisierungen werden grün dargestellt.
- **Fehlgeschlagene Produktausbringungen in den letzten 24 Stunden** – Zeigt ein nach Produkt-Codes gruppiertes Diagramm mit einem Balken an, das alle in den letzten 24 Stunden fehlgeschlagenen Produktausbringungen enthält.
- **Schnelle Systemsuche** – Sie können nach Systemen anhand des Systemnamens, der IP-Adresse, der MAC-Adresse, dem Benutzernamen oder der Agenten-GUID suchen.
- **Fehlgeschlagene Produktaktualisierungen in den letzten 24 Stunden** – Zeigt ein nach Produkt-Codes gruppiertes Diagramm mit einem Balken an, das alle in den letzten 24 Stunden fehlgeschlagenen Produktaktualisierungen enthält.
- **Versuchte Agenten-Deinstallationen in den letzten 7 Tagen** – Zeigt ein nach Tagen gruppiertes Diagramm mit einem Balken an, das alle Agenten-Deinstallationsereignisse auf Clients aus den letzten 7 Tagen enthält.

Festlegen von Standard-Dashboards und Aktualisierungsintervallen für Dashboards

Die Server-Einstellung **Dashboards** gibt das Standard-Dashboard an, das einem Benutzer nach dem Anmelden beim Server angezeigt wird, sowie die Häufigkeit, mit der alle Dashboards aktualisiert werden.

Sie können festlegen, welches Dashboard einem Benutzer nach dem erstmaligen Anmelden beim ePolicy Orchestrator-Server angezeigt werden soll, indem Sie dieses Dashboard dem Berechtigungssatz des Benutzers zuordnen. Durch das Zuordnen von Dashboards zu Berechtigungssätzen wird sichergestellt, dass Benutzern, denen eine bestimmte Rolle zugewiesen wurde, die Informationen angezeigt werden, die sie benötigen. Benutzern, die auch andere Dashboards als ihr Standard-Dashboard anzeigen dürfen, wird beim Wechseln auf die Seite **Dashboards** das Dashboard angezeigt, das sie zuletzt geöffnet hatten.

Mithilfe der Server-Einstellung **Dashboards** können Sie folgende Aktionen durchführen:

- Sie können konfigurieren, welches Dashboard einem Benutzer angezeigt wird, der zu einem Berechtigungssatz gehört, der keine Standard-Dashboard-Zuweisung besitzt.
- Sie können die automatische Aktualisierungsrate für Dashboards steuern.



Dashboards werden automatisch aktualisiert. Bei jedem Aktualisierungsvorgang wird die zugrunde liegende Abfrage ausgeführt, und die Ergebnisse werden im Dashboard angezeigt. Bei Abfrageergebnissen, die große Datenmengen enthalten, kann sich ein kurzes Aktualisierungsintervall negativ auf die verfügbare Bandbreite auswirken. Sie sollten daher ein Aktualisierungsintervall (das standardmäßig 5 Minuten beträgt) wählen, das kurz genug ist, sodass korrekte und aktuelle Informationen angezeigt werden, ohne dass Netzwerkressourcen übermäßig in Anspruch genommen werden.

Vorgehensweise

Definitionen zu Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

1. Klicken Sie auf **Menü** | **Konfiguration** | **Server-Einstellungen**, wählen Sie in der Liste **Einstellungskategorien** den Eintrag **Dashboards** aus, und klicken Sie dann auf **Bearbeiten**.
2. Wählen Sie in den Menüs einen Berechtigungssatz und ein Standard-Dashboard aus.

   Mithilfe der Schaltfläche + und − können Sie bei jedem Berechtigungssatz oder bei Zuweisungen für mehrere Berechtigungssätze mehrere Dashboards hinzufügen oder entfernen.
3. Geben Sie für das Dashboard-Monitor-Aktualisierungsintervall (das standardmäßig 5 Minuten beträgt) einen Wert zwischen 1 Minute und 60 Stunden an, und klicken Sie dann auf **Speichern**.

19 Abfragen und Berichte

ePolicy Orchestrator verfügt über eigene Funktionen für Abfragen und Berichterstellung. Diese sind sehr anpassbar, flexibel und benutzerfreundlich.

Enthalten sind der **Abfragen-Generator** und der **Bericht-Generator**, mit denen sich Abfragen und Berichte erstellen und ausführen lassen, die benutzerkonfigurierte Daten in benutzerkonfigurierten Diagrammen und Tabellen ausgeben. Die Daten für diese Abfragen und Berichte können aus beliebigen registrierten, internen oder externen Datenbanken in Ihrem ePolicy Orchestrator-System stammen.

Zusätzlich zum Abfrage- und Berichterstellungssystem können Sie mithilfe der folgenden Protokolle Informationen zu Aktivitäten erfassen, die auf Ihrem McAfee ePO-Server und in Ihrem Netzwerk stattfinden:

- Audit-Protokoll
- Server-Task-Protokoll
- Bedrohungsereignisprotokoll

Damit Sie sofort mit dem Produkt arbeiten können, hat McAfee eine Reihe von Standardabfragen integriert, die dieselben Informationen liefern wie die Standardberichte in früheren Versionen.

Inhalt

Berechtigungen für Abfragen und Berichte

Es gibt eine Reihe von Möglichkeiten, den Zugriff auf Abfragen und Berichte zu beschränken.

Um eine Abfrage oder einen Bericht auszuführen, benötigen Sie nicht nur für diese Abfrage oder diesen Bericht Berechtigungen, sondern auch für die Funktionssätze, die mit den jeweiligen Ergebnistypen verbundenen sind. Die Ergebnisseiten einer Abfrage bieten nur Zugriff auf Aktionen, die entsprechend Ihren Berechtigungssätzen zugelassen sind.

Gruppen und Berechtigungssätze steuern den Zugriff auf Abfragen und Berichte. Alle Abfragen und Berichte müssen zu einer Gruppe gehören, und der Zugriff auf diese Abfrage bzw. diesen Bericht wird von der Berechtigungsebene der Gruppe gesteuert. Abfrage- und Berichtgruppen können eine der folgenden Berechtigungsebenen haben:

- **Privat** – Die Gruppe ist nur für den Benutzer verfügbar, der sie erstellt hat.
- **Öffentlich** – Die Gruppe ist global freigegeben.
- **Nach Berechtigungssatz** – Die Gruppe ist nur für Benutzer verfügbar, denen die ausgewählten Berechtigungssätze zugewiesen sind.

Berechtigungssätze verfügen über vier Zugriffsebenen für Abfragen oder Berichte. Zu diesen Berechtigungen gehören:

- **Keine Berechtigungen** – Benutzern ohne Berechtigungen wird die Registerkarte **Abfrage** oder **Bericht** nicht angezeigt.
- **Öffentliche Abfragen verwenden** – Gewährt die Berechtigung zum Verwenden aller Abfragen oder Berichte, die in eine **Öffentliche Gruppe** abgelegt wurden.
- **Öffentliche Abfragen verwenden; persönliche Abfragen erstellen und bearbeiten** – Gewährt die Berechtigung zum Verwenden aller Abfragen oder Berichte, die in eine **Öffentliche Gruppe** abgelegt wurden. Außerdem können mit dem **Abfragen-Generator** Abfragen oder Berichte in **Privaten Gruppen** erstellt und bearbeitet werden.
- **Öffentliche Abfragen bearbeiten; persönliche Abfragen erstellen und bearbeiten; persönliche Abfragen veröffentlichen** – Gewährt die Berechtigung zum Verwenden und Bearbeiten aller Abfragen oder Berichte, die in **Öffentlichen Gruppen** abgelegt wurden, sowie zum Erstellen und Bearbeiten von Abfragen oder Berichten in **Privaten Gruppen**. Außerdem können Abfragen oder Berichte von **Privaten Gruppen** in **Öffentliche Gruppen** oder **Freigegebene Gruppen** verschoben werden.

Informationen zu Abfragen

Abfragen sind im Wesentlichen Fragen, die Sie an ePolicy Orchestrator stellen, und die Antworten werden in verschiedenen Diagramm- und Tabellenformen zurückgegeben.

Eine Abfrage kann einzeln verwendet werden, um sofort eine Antwort zu erhalten. Alle Abfrageergebnisse lassen sich in verschiedenen Formaten exportieren, die jeweils heruntergeladen oder als Anhang einer E-Mail-Nachricht gesendet werden können. Die meisten Abfragen können auch als Dashboard-Monitore verwendet werden und ermöglichen dann eine Systemüberwachung in nahezu Echtzeit. Zudem können Abfragen in Berichte aufgenommen werden und bieten dann eine breitere und systematischere Betrachtung Ihres ePolicy Orchestrator-Systems.



Die im Lieferumfang von ePolicy Orchestrator enthaltenen Standard-Dashboards und vordefinierten Abfragen können nicht geändert oder gelöscht werden. Wenn Sie eines dieser Dashboards oder eine dieser Abfragen ändern möchten, müssen Sie es bzw. sie duplizieren und umbenennen. Anschließend können Sie das umbenannte Duplikat ändern.

An Abfrageergebnissen lassen sich Aktionen durchführen

An Abfrageergebnissen lassen sich nun Aktionen durchführen. Für die in Tabellen (und Aufgliederungstabellen) angezeigten Abfrageergebnisse sind bei ausgewählten Elementen in der Tabelle eine Reihe von Aktionen verfügbar. So können Sie beispielsweise Agenten auf Systeme ausbringen, die in einer Tabelle mit Abfrageergebnissen aufgelistet sind. Aktionen stehen unten auf der Ergebnisseite zur Verfügung.

Abfragen als Dashboard-Monitore

Die meisten Abfragen (außer solchen, bei denen die ursprünglichen Ergebnisse mithilfe einer Tabelle angezeigt werden) eignen sich als Dashboard-Monitor. Dashboard-Monitore werden innerhalb benutzerdefinierter Intervalle (Standard sind fünf Minuten) automatisch aktualisiert.

Exportierte Ergebnisse

Abfrageergebnisse lassen sich in vier verschiedenen Formaten exportieren. Bei exportierten Ergebnissen handelt es sich um Verlaufsdaten. Sie werden im Gegensatz zu anderen Monitoren, die als Dashboard-Monitore verwendet werden, nicht aktualisiert. Wie bei den in der Konsole angezeigten Abfrageergebnissen und abfragebasierten Monitoren können Sie HTML-Exporte nach detaillierteren Informationen aufgliedern.

Im Gegensatz zu Abfrageergebnissen in der Konsole sind Daten in exportierten Berichten nicht für Aktionen geeignet.

Berichte stehen in verschiedenen Formaten zur Verfügung:

- CSV – Verwenden Sie dieses Format, um die Daten in einer Tabellenkalkulationsanwendung (z. B. Microsoft Excel) zu verwenden.
- XML – Verwenden Sie dieses Format, um die Daten für andere Zwecke zu transformieren.
- HTML – Verwenden Sie dieses Format, um die exportierten Ergebnisse als Webseite anzuzeigen.
- PDF – Verwenden Sie dieses Format, wenn Sie die Ergebnisse ausdrucken möchten.

Einbinden von Abfragen in Berichte

Berichte können beliebig viele Abfragen, Bilder, statische Texte und andere Elemente enthalten. Sie können bei Bedarf oder nach einem regelmäßigen Zeitplan ausgeführt werden und werden für eine Anzeige außerhalb von ePolicy Orchestrator als PDF-Datei ausgegeben.

Freigeben von Abfragen zwischen Servern

Jede Abfrage kann importiert und exportiert werden. Hierdurch können Sie Abfragen zwischen Servern freigeben. Dadurch müssen Abfragen in Umgebungen mit mehreren Servern nur einmal erstellt werden.

Abrufen von Daten aus unterschiedlichen Quellen

Abfragen können Daten von jedem registrierten Server abrufen, auch von ePolicy Orchestrator-externen Datenbanken.

Abfragen-Generator

ePolicy Orchestrator enthält einen einfachen Assistenten, mit dem Sie benutzerdefinierte Abfragen in vier Schritten erstellen und bearbeiten können. Mit dem Assistenten können Sie konfigurieren, welche Daten abgerufen und angezeigt werden. Darüber hinaus können Sie angeben, in welcher Form sie angezeigt werden.

Ergebnistypen

Als erstes wählen Sie im Abfragen-Generator das Schema und den Ergebnistyp aus einer Funktionsgruppe aus. Damit geben Sie an, woher die Abfrage Daten abruft, welcher Typ von Daten abgerufen wird und welche weiteren Auswahlmöglichkeiten auf den restlichen Seiten des Assistenten zur Verfügung stehen.

Diagrammtypen

ePolicy Orchestrator verfügt über eine Reihe von Diagrammen und Tabellen zum Anzeigen der abgerufenen Daten. Diese Diagramme und Tabellen und deren Aufgliederungstabellen sind in hohem Maße konfigurierbar.



Aufgliederungstabellen gehören nicht zu den Tabellen.

Zu den Diagrammtypen gehören:

Tabelle 19-1 Diagrammtypgruppen

Typ	Diagramm oder Tabelle
Balken	• Balkendiagramm • Diagramm mit gruppierten Balken • Gestapeltes Balkendiagramm
Kreis	• Boolesches Kreisdiagramm • Kreisdiagramm
Blase	• Blasendiagramm
Zusammenfassung	• Gruppierte Übersichtstabelle mit mehreren Gruppen • Gruppierte Übersichtstabelle mit einer Gruppe
Linie	• Diagramm mit mehreren Linien • Diagramm mit einer Linie
Liste	• Tabelle

Tabellenspalten

Geben Sie Spalten für die Tabelle an. Wenn Sie **Tabelle** als primäre Ansicht der Daten auswählen, wird diese Tabelle konfiguriert. Wenn Sie als erste Ansicht der Daten einen Diagrammtyp auswählen, wird die Aufgliederungstabelle konfiguriert.

An den in einer Tabelle angezeigten Abfrageergebnisse lassen sich Aktionen durchführen. Wenn die Tabelle beispielsweise mit Systemen aufgefüllt ist, können Sie Agenten für diese Systeme direkt aus der Tabelle ausbringen oder reaktivieren.

Filter

Legen Sie durch Auswählen von Eigenschaften und Operatoren spezielle Kriterien fest, um die von der Abfrage abgerufenen Daten einzuschränken.

Erstmaliges Konfigurieren von Abfragen und Berichten

Gehen Sie wie nachfolgend allgemein beschrieben vor, wenn Sie zum ersten Mal Abfragen und Berichte konfigurieren.

1. Machen Sie sich mit den Funktionen von Abfragen, Berichten und dem Abfragen-Generator vertraut.
2. Sehen Sie sich die Standardabfragen und -berichte an, und bearbeiten Sie sie nach Bedarf.
3. Erstellen Sie Abfragen und Berichte für alle Anforderungen, die durch die Standardabfragen nicht abgedeckt werden.

Arbeiten mit Abfragen

Abfragen können je nach Ihren Anforderungen u. a. erstellt, ausgeführt, exportiert und dupliziert werden.

Aufgaben

- *Verwalten benutzerdefinierter Abfragen* auf Seite 265
  Sie können Abfragen nach Bedarf erstellen, duplizieren, bearbeiten und löschen.
- *Ausführen einer vorhandenen Abfrage* auf Seite 267
  Sie können gespeicherte Abfragen bei Bedarf ausführen.
- *Planmäßiges Ausführen einer Abfrage* auf Seite 267
  Zum regelmäßigen Ausführen einer Abfrage wird ein Server-Task verwendet.
- *Erstellen einer Abfragegruppe* auf Seite 268
  Mithilfe von Abfragegruppen können Sie Abfragen oder Berichte speichern, ohne anderen Benutzern den Zugriff darauf zu erlauben.
- *Verschieben einer Abfrage in eine andere Gruppe* auf Seite 268
  Sie können die Berechtigungen für eine Abfrage ändern, indem Sie die Abfrage in eine andere Gruppe verschieben.
- *Exportieren und Importieren von Abfragen* auf Seite 269
  Um sicherzustellen, dass unterschiedliche ePolicy Orchestrator-Server Daten auf die gleiche Weise abrufen, können Abfragen exportiert und importiert werden.
- *Exportieren von Abfrageergebnissen in andere Formate* auf Seite 270
  Abfrageergebnisse können in viele unterschiedliche Formate, wie HTML, PDF, CSV und XML, exportiert werden.

Verwalten benutzerdefinierter Abfragen

Sie können Abfragen nach Bedarf erstellen, duplizieren, bearbeiten und löschen.

Vorgehensweise

Definitionen zu Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

1. Klicken Sie auf **Menü** | **Berichterstellung** | **Abfragen und Berichte**. Die Seite **Abfragen und Berichte** wird angezeigt.
2. Wählen Sie eine der folgenden Aktionen aus.

<table>
<tr><th>Aktion</th><th>Vorgehensweise</th></tr>
<tr><td>Erstellen von benutzerdefinierten Abfragen</td><td>
1 Klicken Sie auf **Aktionen** | **Neu**. Der **Abfragen-Generator** wird angezeigt.
2 Wählen Sie auf der Seite **Ergebnistyp** die **Funktionsgruppe** und den **Ergebnistyp** für diese Abfrage aus, und klicken Sie dann auf **Weiter**.
3 Wählen Sie den Typ von Diagramm oder Tabelle aus, mit dem die primären Ergebnisse der Abfrage dargestellt werden sollen, und klicken Sie dann auf **Weiter**.
Wenn Sie **Boolesches Kreisdiagramm** auswählen, müssen Sie noch die Kriterien konfigurieren, die in der Abfrage enthalten sein sollen.
4 Wählen Sie die Spalten aus, die in der Abfrage enthalten sein sollen, und klicken Sie dann auf **Weiter**.
Wenn Sie auf der Seite **Diagramm** die Option **Tabelle** ausgewählt haben, bilden die von Ihnen hier ausgewählten Spalten die Spalten dieser Tabelle. Andernfalls bilden diese Spalten die Abfragedetails-Tabelle.
5 Wählen Sie Eigenschaften aus, um die Suchergebnisse einzugrenzen, und klicken Sie dann auf **Ausführen**. Auf der Seite **Ungespeicherte Abfrage** werden die Ergebnisse der Abfrage angezeigt, an denen sich Aktionen durchführen lassen. Sie können daher alle verfügbaren Aktionen für Elemente in sämtlichen Tabellen oder Aufgliederungstabellen durchführen.
Ausgewählte Eigenschaften werden im Inhaltsbereich mit Operatoren angezeigt, die Kriterien festlegen können, nach denen die für die jeweilige Eigenschaft zurückgegebenen Daten eingegrenzt werden.
• Wenn die Abfrage nicht die erwarteten Ergebnisse zurückgegeben hat, klicken Sie auf **Abfrage bearbeiten**, um zurück zum **Abfragen-Assistenten** zu wechseln und die Details der Abfrage zu bearbeiten.
• Wenn Sie die Abfrage nicht speichern möchten, klicken Sie auf **Schließen**.
• Wenn Sie diese Abfrage zu einem späteren Zeitpunkt erneut verwenden möchten, klicken Sie auf **Speichern**, und fahren mit dem nächsten Schritt fort.
6 Die Seite **Abfrage speichern** wird angezeigt. Geben Sie einen Namen für die Abfrage ein, fügen Sie Anmerkungen hinzu, und wählen Sie eine der folgenden Optionen aus:
• **Neue Gruppe** – Geben Sie den Namen der neuen Gruppe ein, und wählen Sie eine der folgenden Optionen:
  • **Private Gruppe (Eigene Gruppen)**
  • **Öffentliche Gruppe (Freigegebene Gruppen)**
• **Vorhandene Gruppe** – Wählen Sie die Gruppe in der Liste **Freigegebene Gruppen** aus.
7 Klicken Sie auf **Speichern**.
Die neue Abfrage wird in der Liste **Abfragen** angezeigt.
</td></tr>
<tr><td>Duplizieren von Abfragen</td><td>1 Wählen Sie in der Liste die Abfrage aus, die dupliziert werden soll, und klicken Sie auf **Aktionen** | **Duplizieren**.</td></tr>
</table>

Aktion	Vorgehensweise
	2 Geben Sie im Dialogfeld **Duplizieren** einen Namen für das Duplikat ein, und wählen Sie eine Gruppe aus, die eine Kopie der Abfrage erhalten soll. Klicken Sie anschließend auf **OK**. Die duplizierte Abfrage wird in der Liste **Abfragen** angezeigt.
Bearbeiten von Abfragen	1 Wählen Sie in der Liste die Abfrage aus, die bearbeitet werden soll, und klicken Sie dann auf **Aktionen** | **Bearbeiten**. Der **Abfragen-Generator** wird mit der Startseite **Diagrammtyp** angezeigt. 2 Bearbeiten Sie die Einstellungen der Abfrage, und klicken Sie dann auf **Speichern**. Die Abfrage wird mit den vorgenommenen Änderungen in der Liste **Abfragen** angezeigt.
Löschen von Abfragen	1 Wählen Sie in der Liste die Abfrage aus, die gelöscht werden soll, und klicken Sie auf **Aktionen** | **Löschen**. 2 Klicken Sie im angezeigten Bestätigungsdialogfeld auf **Ja**. Die Abfrage wird nicht mehr in der Liste **Abfragen** angezeigt. Berichte oder Server-Tasks, in denen die gelöschte Abfrage verwendet wurde, werden so lange als ungültig angezeigt, bis in ihnen der Verweis auf die gelöschte Abfrage entfernt wird.

Ausführen einer vorhandenen Abfrage

Sie können gespeicherte Abfragen bei Bedarf ausführen.

Vorgehensweise

Definitionen zu Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

1. Klicken Sie auf **Menü** | **Berichterstellung** | **Abfragen und Berichte**, und wählen Sie dann eine Abfrage in der Liste **Abfragen** aus.
2. Klicken Sie auf **Aktionen** | **Ausführen**. Die Ergebnisse der Abfrage werden angezeigt. Sie können den Bericht weiter aufgliedern und nach Bedarf Aktionen an Elementen durchführen.

   Welche Aktionen verfügbar sind, hängt von den Berechtigungen des Benutzers ab.
3. Klicken Sie auf **Schließen**, wenn Sie alle gewünschten Vorgänge durchgeführt haben.

Planmäßiges Ausführen einer Abfrage

Zum regelmäßigen Ausführen einer Abfrage wird ein Server-Task verwendet.
Definitionen zu Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

Vorgehensweise

1. Klicken Sie auf **Menü** | **Automatisierung** | **Server-Tasks**, und klicken Sie dann auf **Aktionen** | **Neuer Task**.
2. Geben Sie auf der Seite **Beschreibung** einen Namen und eine Beschreibung für den Task ein, und klicken Sie dann auf **Weiter**.
3. Wählen Sie im Dropdown-Menü **Aktionen** den Eintrag **Abfrage ausführen** aus.
4. Suchen Sie im Feld **Abfrage** die Abfrage, die Sie ausführen möchten.
5. Wählen Sie die Sprache aus, in der die Ergebnisse angezeigt werden sollen.

6 Wählen Sie in der Liste **Untergeordnete Aktionen** eine Aktion aus, die basierend auf den Ergebnissen ausgeführt werden soll. Welche Aktionen verfügbar sind, hängt von den Berechtigungen des Benutzers und den vom ePolicy Orchestrator-Server verwalteten Produkten ab.



Sie können auch mehrere Aktionen für die Abfrageergebnisse auswählen. Klicken Sie auf die Schaltfläche **+**, um weitere Aktionen hinzuzufügen, die an den Abfrageergebnissen durchgeführt werden sollen. Achten Sie dabei darauf, dass Sie die Aktionen in der Reihenfolge anordnen, in der sie an den Abfrageergebnissen durchgeführt werden sollen.

7 Klicken Sie auf **Weiter**.

8 Planen Sie den Task nach Bedarf, und klicken Sie dann auf **Weiter**.

9 Überprüfen Sie die Konfiguration des Tasks, und klicken Sie dann auf **Speichern**.

Der Task wird zur Liste auf der Seite **Server-Tasks** hinzugefügt. Wenn der Task aktiviert ist (Standardeinstellung), wird er zum nächsten geplanten Zeitpunkt ausgeführt. Ist der Task deaktiviert, wird er nur dann ausgeführt, wenn Sie auf der Seite **Server-Tasks** neben dem Task auf **Ausführen** klicken.

Erstellen einer Abfragegruppe

Mithilfe von Abfragegruppen können Sie Abfragen oder Berichte speichern, ohne anderen Benutzern den Zugriff darauf zu erlauben.

Durch Erstellen einer Gruppe können Sie Abfragen und Berichte nach ihrer Funktion kategorisieren und den Zugriff auf diese Elemente steuern. Die in ePolicy Orchestrator angezeigte Liste von Gruppen enthält sowohl die von Ihnen erstellten Gruppen als auch die, für die Sie Anzeigeberechtigungen besitzen.



Beim Speichern einer benutzerdefinierten Abfrage können Sie auch private Abfragegruppen erstellen.

Vorgehensweise

Definitionen zu Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

1 Klicken Sie auf **Menü** | **Berichterstellung** | **Abfragen und Berichte**, und klicken Sie dann auf **Gruppenaktionen** | **Neue Gruppe**.

2 Geben Sie auf der Seite **Neue Gruppe** einen Gruppennamen ein.

3 Wählen Sie in **Gruppensichtbarkeit** eine der folgenden Optionen aus:

- **Private Gruppe** – Fügt die neue Gruppe unter **Eigene Gruppen** hinzu.
- **Öffentliche Gruppe** – Fügt die neue Gruppe unter **Freigegebene Gruppen** hinzu. In dieser Gruppe enthaltene Abfragen und Berichte können allen Benutzern angezeigt werden, die über Zugriff auf öffentliche Abfragen und Berichte verfügen.
- **Nach Berechtigungssatz freigegeben** – Fügt die neue Gruppe unter **Freigegebene Gruppen** hinzu. Auf Abfragen und Berichte in dieser Gruppe können nur Benutzer zugreifen, die den ausgewählten Berechtigungssätzen zugewiesen wurden.



Administratoren haben vollständigen Zugriff auf alle Abfragen vom Typ **Nach Berechtigungssatz** und **Öffentliche Gruppe**.

4 Klicken Sie auf **Speichern**.

Verschieben einer Abfrage in eine andere Gruppe

Sie können die Berechtigungen für eine Abfrage ändern, indem Sie die Abfrage in eine andere Gruppe verschieben.

Vorgehensweise

Definitionen zu Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

1. Klicken Sie auf **Menü** | **Berichterstellung** | **Abfragen und Berichte**. Wählen Sie in der Liste **Abfragen** die Abfrage aus, die Sie verschieben möchten.
2. Klicken Sie auf **Aktionen**, und wählen Sie eine der folgenden Optionen aus:
   - **In andere Gruppe verschieben** – Wählen Sie die gewünschte Gruppe im Menü **Zielgruppe auswählen** aus.
   - **Duplizieren** – Geben Sie einen neuen Namen an, und wählen Sie die gewünschte Gruppe im Menü **Gruppe, die Kopie erhält** aus.
3. Klicken Sie auf **OK**.

Exportieren und Importieren von Abfragen

Um sicherzustellen, dass unterschiedliche ePolicy Orchestrator-Server Daten auf die gleiche Weise abrufen, können Abfragen exportiert und importiert werden.

Vorgehensweise

Definitionen zu Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

1. Öffnen Sie die Seite **Abfragen**, indem Sie auf **Menü** | **Berichterstellung** | **Abfragen und Berichte** klicken und dann die Registerkarte **Abfrage** auswählen.
2. Wählen Sie eine der folgenden Aktionen aus.

Aktion	Vorgehensweise
Exportieren von Abfragen	1 Wählen Sie in der Liste **Gruppen** die Gruppe aus, in der sich die Abfrage befindet, die Sie exportieren möchten, und wählen Sie dann die zu exportierende Abfrage aus. 2 Klicken Sie auf **Aktionen | Definitionen exportieren**. Der McAfee ePO-Server sendet eine XML-Datei an Ihren Browser. Der nächste Schritt hängt von Ihren Browser-Einstellungen ab. Von den meisten Browsern werden Sie standardmäßig zum Speichern der Datei aufgefordert. Die exportierte XML-Datei enthält eine vollständige Beschreibung aller Einstellungen, die zum Replizieren der exportierten Abfrage erforderlich sind.
Importieren von Abfragen	1 Klicken Sie auf **Aktionen | Definitionen importieren**. 2 Klicken Sie auf **Durchsuchen**, und wählen Sie die XML-Datei aus, in der sich der zu importierende Bericht befindet. 3 Wählen Sie eine neue oder eine vorhandene Gruppe für die Abfrage aus. Wenn es sich um eine neue Gruppe handelt, geben Sie einen Namen für die Gruppe ein, und wählen Sie aus, ob sie privat oder öffentlich ist. Bei einer vorhandenen Gruppe wählen Sie die Gruppe für die importierte Abfrage aus. 4 Klicken Sie auf **Speichern**. Es wird ein Bestätigungsbildschirm mit den Informationen zu der Abfrage aus der XML-Datei und ihrer Benennung nach dem Import angezeigt. Wenn die ausgewählte Datei keine gültige Abfrage enthält, wird eine Fehlermeldung angezeigt. 5 Klicken Sie auf **OK**, um den Importvorgang abzuschließen. Der neu importierten Abfrage werden die Berechtigungen der Gruppe zugewiesen, in die sie importiert wurde.

Exportieren von Abfrageergebnissen in andere Formate

Abfrageergebnisse können in viele unterschiedliche Formate, wie HTML, PDF, CSV und XML, exportiert werden.

Das Exportieren von Abfrageergebnissen unterscheidet sich in mehreren Punkten vom Erstellen eines Berichts. Erstens werden zu der Ausgabe keine zusätzlichen Informationen hinzugefügt, wie es bei einem Bericht möglich ist. Eine Abfrage enthält nur die Ergebnisdaten. Außerdem werden mehrere Formate unterstützt. Es wird davon ausgegangen, dass exportierte Abfrageergebnisse weiter verarbeitet werden, deshalb werden Formate wie XML und CSV unterstützt. Berichte müssen vom Benutzer lesbar sein und werden daher nur als PDF-Dateien ausgegeben.

Im Gegensatz zu Abfrageergebnissen in der Konsole sind exportierte Daten nicht für Aktionen geeignet.

Vorgehensweise

Definitionen zu Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

1 Klicken Sie auf **Menü | Berichterstellung | Abfragen und Berichte**, und wählen Sie dann mindestens eine Abfrage aus.



Sie können die Abfrage auch auf der Seite **Abfragen** ausführen und auf der Ergebnisseite auf **Optionen | Daten exportieren** klicken, um die Seite **Exportieren** zu öffnen.

2. Klicken Sie auf **Aktionen** | **Daten exportieren**.

   Die Seite **Exportieren** wird angezeigt.

3. Wählen Sie aus, welche Elemente exportiert werden soll. Wählen Sie für diagrammbasierte Abfragen entweder **Nur Diagrammdaten** oder **Diagrammdaten und Aufgliederungstabellen** aus.

4. Legen Sie fest, ob die Datendateien einzeln oder in einer einzigen Archivdatei (ZIP) exportiert werden sollen.

5. Wählen Sie das Format der exportierten Datei aus.
   - **CSV** – Verwenden Sie dieses Format, um die Daten in einer Tabellenkalkulationsanwendung (z. B. Microsoft Excel) zu verwenden.
   - **XML** – Verwenden Sie dieses Format, um die Daten für andere Zwecke zu transformieren.
   - **HTML** – Verwenden Sie dieses Format, um die exportierten Ergebnisse als Webseite anzuzeigen.
   - **PDF** – Verwenden Sie dieses Format, wenn Sie die Ergebnisse ausdrucken möchten.

6. Wenn Sie in eine PDF-Datei exportieren, müssen Sie Folgendes konfigurieren:
   - Wählen Sie die **Seitengröße** und die **Seitenausrichtung** aus.
   - (Optional) **Filterkriterien anzeigen**.
   - (Optional) **Deckblatt mit folgendem Text hinzufügen**. Geben Sie den gewünschten Text ein.

7. Legen Sie fest, ob die Dateien als E-Mail-Anhänge an ausgewählte Empfänger gesendet oder in einem Speicherort auf dem Server gespeichert werden sollen, für den ein Link bereitgestellt wird. Die Datei können Sie öffnen oder an einem anderen Ort speichern, indem Sie mit der rechten Maustaste darauf klicken.

   Beim Eingeben mehrerer E-Mail-Adressen für Empfänger müssen Sie die Einträge mit einem Komma oder Semikolon trennen.

8. Klicken Sie auf **Exportieren**.

Die Dateien werden erstellt und entweder als E-Mail-Anhänge an die Empfänger gesendet, oder es wird eine Seite aufgerufen, auf der Sie über Links auf die Dateien zugreifen können.

Zusammengefasste Abfragen mehrerer Server

ePolicy Orchestrator bietet die Möglichkeit zur Ausführung von Abfragen, bei denen ein Bericht mit einer Zusammenfassung von Daten aus mehreren Datenbanken erstellt wird.

Verwenden Sie diese Ergebnistypen im **Abfragen-Generator** für Abfragen dieses Typs:

- Zusammengefasste Bedrohungsereignisse
- Client-Ereignisse mit zusammengefassten Daten
- Compliance-Verlauf mit zusammengefassten Daten
- Verwaltete Systeme mit zusammengefassten Daten
- Zusammengefasste angewendete Richtlinien

Aktionsbefehle können nicht aus Ergebnistypen mit zusammengefassten Daten generiert werden.

Vorgehensweise

Zum Zusammenfassen von Daten, die in Abfragen mit zusammengefassten Daten verwendet werden sollen, müssen Sie jeden Server (einschließlich des lokalen Servers) registrieren, den Sie in die Abfrage einbeziehen möchten.

Nach der Registrierung der Server müssen Sie auf dem Berichterstellungs-Server (dem Server, auf dem die Berichterstellung für mehrere Server durchgeführt wird) Server-Tasks zum Zusammenfassen von Daten konfigurieren. Server-Tasks zum Zusammenfassen von Daten rufen Informationen aus allen in den Bericht einfließenden Datenbanken ab und füllen die "EPORollup_"-Tabellen auf dem Berichterstellungs-Server auf. Die Abfragen mit zusammengefassten Daten haben diese Datenbanktabellen auf dem Berichterstellungs-Server zum Ziel.



Vor dem Ausführen einer Compliance-Verlaufsabfrage mit zusammengefassten Daten müssen Sie auf jedem Server, dessen Daten in der Abfrage enthalten sein sollen, zwei vorbereitende Schritte ausführen:

- Erstellen einer Abfrage zum Definieren der Compliance
- Generieren eines Compliance-Ereignisses

Erstellen eines Server-Tasks zum Zusammenfassen von Daten

Server-Tasks zum Zusammenfassen von Daten beziehen Daten aus mehreren Servern gleichzeitig.

Bevor Sie beginnen

ePolicy Orchestrator-Berichterstellungs-Server, die in Zusammenfassungsberichten enthalten sein sollen, müssen Sie zuvor registrieren. Die Server müssen registriert werden, um von diesen Servern zusammengefasste Daten zu sammeln, mit denen die "EPORollup_"-Tabellen des Zusammenfassungs-Berichterstellungs-Servers aufgefüllt werden.



Der Berichterstellungs-Server muss ebenfalls registriert werden, wenn seine zusammengefassten Daten in der Berichterstellung mit zusammengefassten Daten enthalten sein sollen.

Vorgehensweise

Definitionen zu Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

1. Klicken Sie auf **Menü** | **Automatisierung** | **Server-Tasks**, und klicken Sie dann auf **Aktionen** | **Neuer Task**.
2. Geben Sie auf der Seite **Beschreibung** einen Namen und eine Beschreibung für den Task ein, und legen Sie fest, ob er aktiviert werden soll. Klicken Sie anschließend auf **Weiter**.
3. Klicken Sie auf **Aktionen**, und wählen Sie **Daten zusammenfassen** aus.
4. Wählen Sie im Dropdown-Menü **Daten zusammenfassen von:** entweder **Allen registrierten Servern** oder **Ausgewählten registrierten Servern** aus.
5. Wenn Sie im vorherigen Schritt den Eintrag **Registrierte Server auswählen** ausgewählt haben, klicken Sie auf **Auswählen**, und wählen Sie die Server aus, von denen Daten im Dialogfeld **Registrierte Server auswählen** zusammengefasst werden sollen. Klicken Sie auf **OK**.

6 Wählen Sie die Datentypen aus, die zusammengefasst werden sollen. Wenn Sie mehrere Datentypen auswählen möchten, klicken Sie auf das Pluszeichen (**+**) am Ende der Tabellenüberschrift.



Die Datentypen "Bedrohungsereignisse", "Client-Ereignisse" und "Angewendete Richtlinien" können noch weiter konfiguriert werden, sodass sie die zusätzlichen Eigenschaften "Bereinigen", "Filter" und "Zusammenfassungsmethode" enthalten. Klicken Sie dazu in der Zeile, in der die zusätzlichen verfügbaren Eigenschaften beschrieben sind, auf **Konfigurieren**.

7 Klicken Sie auf **Weiter**.

Die Seite **Plan** wird angezeigt.

8 Planen Sie den Task, und klicken Sie dann auf **Weiter**.

Die Seite **Zusammenfassung** wird angezeigt.



Falls Sie Berichte zu zusammengefassten Compliance-Verlaufs-Daten erstellen, vergewissern Sie sich, dass die Zeiteinheit der Abfrage "Compliance-Verlauf mit zusammengefassten Daten" dem Planungstyp der Server-Tasks "Compliance-Ereignis generieren" auf den registrierten Servern entspricht.

9 Überprüfen Sie die Einstellungen, und klicken Sie dann auf **Speichern**.

Erstellen einer Abfrage zum Definieren der Compliance

Compliance-Abfragen sind auf McAfee ePO-Servern erforderlich, deren Daten in Abfragen mit zusammengefassten Daten verwendet werden.

Vorgehensweise

Definitionen zu Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

1 Klicken Sie auf **Menü** | **Berichterstellung** | **Abfragen und Berichte**, und klicken Sie dann auf **Aktionen** | **Neu**.

2 Wählen Sie auf der Seite **Ergebnistyp** als Funktionsgruppe **Systemverwaltung** aus, wählen Sie als Ergebnistypen **Verwaltete Systeme** aus, und klicken Sie dann auf **Weiter**.

3 Wählen Sie in der Liste **Ergebnisse anzeigen als** die Option **Boolesches Kreisdiagramm** aus, und klicken Sie anschließend auf **Kriterien konfigurieren**.

4 Wählen Sie die in die Abfrage einzuschließenden Eigenschaften aus, und legen Sie dann die Operatoren und Werte für jede Eigenschaft fest. Klicken Sie auf **OK**. Wenn die Seite **Diagramm** angezeigt wird, klicken Sie auf **Weiter**.



Diese Eigenschaften bestimmen, was für Systeme konform ist, die von diesem McAfee ePO-Server verwaltet werden.

5 Wählen Sie die Spalten aus, die in der Abfrage enthalten sein sollen, und klicken Sie dann auf **Weiter**.

6 Wählen Sie die Filter für diese Abfrage aus, klicken Sie auf **Ausführen** und anschließend auf **Speichern**.

Generieren von Compliance-Ereignissen

Compliance-Ereignisse werden in Abfragen mit zusammengefassten Daten verwendet, um Daten in einem Bericht zu aggregieren.

Vorgehensweise

Definitionen zu Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

1. Klicken Sie auf **Menü** | **Automatisierung** | **Server-Tasks**, und klicken Sie dann auf **Aktionen** | **Neuer Task**.
2. Geben Sie auf der Seite **Beschreibung** einen Namen für den neuen Task ein, und klicken Sie anschließend auf **Weiter**.
3. Wählen Sie im Dropdown-Menü **Aktionen** den Eintrag **Abfrage ausführen** aus.
4. Klicken Sie neben dem Feld **Abfrage** auf die Schaltfläche zum Durchsuchen […], und wählen Sie eine Abfrage aus. Das Dialogfeld **Wählen Sie eine Abfrage in der Liste aus** wird angezeigt, und die Registerkarte **Private Gruppen** ist aktiv.
5. Wählen Sie die Abfrage aus, durch die die Compliance definiert wird. Es sollte sich dabei um eine Standardabfrage handeln, z. B. **Compliance-Übersicht von McAfee Agent** auf der Registerkarte **McAfee-Gruppen**, oder um eine vom Benutzer erstellte Abfrage, z. B. wie unter *Erstellen einer Abfrage zum Definieren der Compliance* beschrieben.
6. Wählen Sie im Dropdown-Menü **Untergeordnete Aktionen** die Option **Compliance-Ereignis generieren** aus, geben Sie den Prozentsatz oder die Anzahl der Zielsysteme an, und klicken Sie dann auf **Weiter**.

   Ereignisse können mit dem Task "Compliance-Ereignis generieren" generiert werden, wenn die Non-Compliance einen festgelegten Prozentsatz oder eine festgelegte Anzahl von Systemen übersteigt.

7. Planen Sie den Task für das erforderliche Zeitintervall zum Erstellen des Berichts **Compliance-Verlauf** ein. Wenn die Compliance zum Beispiel wöchentlich erfasst werden muss, planen Sie den Task zur wöchentlichen Ausführung. Klicken Sie auf **Weiter**.
8. Prüfen Sie die Angaben, und klicken Sie auf **Speichern**.

Informationen zu Berichten

Berichte fassen Abfragen und andere Elemente in PDF-Dokumenten zusammen und stellen somit detaillierte Informationen für Analysen bereit.

Sie führen Berichte aus, um den Zustand Ihrer Umgebung zu ermitteln (z. B. Schwachstellen, Auslastung, Ereignisse usw.), sodass Sie die erforderlichen Änderungen vornehmen können, damit Ihre Umgebung sicher bleibt.

Abfragen stellen ähnliche Informationen bereit, können jedoch nur bei direkter Interaktion mit einem ePolicy Orchestrator-Server verwendet werden. In Berichten können Sie Informationen aus einer oder mehreren Abfragen in einem einzigen PDF-Dokument bündeln, wodurch eine zielgerichtete Analyse offline ermöglicht wird.

Als konfigurierbare Dokumente zeigen Berichte die Daten aus Abfragen von einer oder mehreren Datenbanken an. Im System wird jeweils das neueste Ergebnis für jeden Bericht gespeichert und zum Anzeigen zur Verfügung gestellt.

Den Zugriff auf Berichte können Sie mithilfe von Gruppen und Berechtigungssätzen auf die gleiche Weise wie bei Abfragen beschränken. Für Berichte und Abfragen können dieselben Gruppen verwendet werden, und da Berichte vor allem aus Abfragen bestehen, ist dadurch eine konsistente Zugriffssteuerung möglich.

Struktur von Berichten

Berichte enthalten eine Reihe von Elementen in einem Grundformat.

Auch wenn Berichte in hohem Maße angepasst werden können, weisen sie eine Grundstruktur auf, die die verschiedenen Elemente enthält.

Seitengröße und -ausrichtung

ePolicy Orchestrator unterstützt derzeit sechs Kombinationen von Seitengröße und -ausrichtung. Dazu gehören:

Seitengröße:

- US Letter (216 x 279 mm)
- US Legal (216 x 356 mm)
- A4 (210 x 297 mm)

Ausrichtung:

- Querformat
- Hochformat

Kopf- und Fußzeilen

Kopf- und Fußzeilen können ebenfalls in der Standardeinstellung verwendet oder vom Benutzer angepasst werden, auch mit Logos. Derzeit für Kopf- und Fußzeilen unterstützte Elemente sind:

- Logo
- Datum/Uhrzeit
- Seitennummer
- Benutzername
- Benutzerdefinierter Text

Seitenelemente

Seitenelemente bilden den Inhalt des Berichts. Sie können in beliebiger Reihenfolge kombiniert und nach Bedarf dupliziert werden. In ePolicy Orchestrator bereitgestellte Seitenelemente sind:

- Bilder
- Statischer Text
- Seitenumbrüche
- Abfragetabellen
- Abfragediagramme

Arbeiten mit Berichten

Berichte, die Abfragen und andere Elemente in detaillierten PDF-Dokumenten zusammenfassen, können erstellt, bearbeitet und verwaltet werden.

Diese Dokumente können eine große Menge nützlicher Daten liefern. Es sind jedoch einige Schritte erforderlich, um eine für Sie hilfreiche Datensammlung zu erstellen.

Aufgaben

- *Erstellen eines neuen Berichts* auf Seite 276
  Sie können neue Berichte erstellen und diese in ePolicy Orchestrator speichern.
- *Bearbeiten eines vorhandenen Berichts* auf Seite 277
  Sie können den Inhalt oder die Präsentationsreihenfolge eines vorhandenen Berichts ändern.
- *Anzeigen von Berichtergebnissen* auf Seite 282
  Sie können für jeden Bericht die zuletzt ausgeführte Version anzeigen.
- *Gruppieren von Berichten* auf Seite 282
  Jeder Bericht muss einer Gruppe zugewiesen sein.
- *Ausführen von Berichten* auf Seite 282
  Bevor Ergebnisse angezeigt werden können, müssen Berichte ausgeführt werden.
- *Ausführen eines Berichts mit einem Server-Task* auf Seite 283
  Mithilfe von Server-Tasks können Berichte automatisch ausgeführt werden.
- *Exportieren und Importieren von Berichten* auf Seite 283
  Da Berichte mitunter sehr detaillierte Informationen enthalten, kann durch Exportieren und Importieren von einem Server auf einen anderen sichergestellt werden, dass der Datenabruf und die Berichterstellung auf allen ePolicy Orchestrator-Servern konsistent erfolgt.
- *Konfigurieren der Vorlage und des Speicherorts für exportierte Berichte* auf Seite 284
  Sie können das Erscheinungsbild und den Speicherort für Tabellen und Dashboards definieren, die Sie als Dokumente exportieren.
- *Löschen von Berichten* auf Seite 285
  Nicht mehr benötigte Berichte können gelöscht werden.
- *Konfigurieren von Internet Explorer 8 zum automatischen Akzeptieren von McAfee ePO-Downloads* auf Seite 285
  Automatisch stattfindende Downloads von ePolicy Orchestrator können aus Sicherheitsgründen von Microsoft Internet Explorer blockiert werden. Dieses Verhalten können Sie durch eine Konfigurationsänderung in Internet Explorer ändern.

Erstellen eines neuen Berichts

Sie können neue Berichte erstellen und diese in ePolicy Orchestrator speichern.

Vorgehensweise

Definitionen zu Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

1. Klicken Sie auf **Menü** | **Berichterstellung** | **Abfragen und Berichte**, und wählen Sie dann die Registerkarte **Bericht** aus.
2. Klicken Sie auf **Aktionen** | **Neu**.

   Eine Seite mit einem leeren **Bericht-Layout** wird angezeigt.
3. Klicken Sie auf **Name, Beschreibung und Gruppe**. Geben Sie einen Namen und optional eine Beschreibung für den Bericht ein, und wählen Sie eine geeignete Gruppe für ihn aus. Klicken Sie auf **OK**.
4. Nun können Sie Elemente hinzufügen, entfernen und neu anordnen, Kopf- und Fußzeilen anpassen und das Seitenlayout ändern. Sie können jederzeit Ihren Fortschritt überprüfen, indem Sie auf **Ausführen** klicken, um den Bericht auszuführen.
5. Klicken Sie abschließend auf **Speichern**.

Bearbeiten eines vorhandenen Berichts

Sie können den Inhalt oder die Präsentationsreihenfolge eines vorhandenen Berichts ändern.

Wenn Sie einen neuen Bericht erstellen, gelangen Sie durch Klicken auf **Neuer Bericht** zu diesem Bildschirm.

Vorgehensweise

Definitionen zu Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

1. Klicken Sie auf **Menü** | **Berichterstellung** | **Abfragen und Berichte**, und wählen Sie dann die Registerkarte **Bericht** aus.
2. Wählen Sie in der Liste einen Bericht aus, indem Sie das Kontrollkästchen neben dem entsprechenden Namen aktivieren.
3. Klicken Sie auf **Bearbeiten**.

   Die Seite **Bericht-Layout** wird angezeigt.

Die folgenden Aufgaben können nun an dem Bericht durchgeführt werden.

Aufgaben

- *Hinzufügen von Elementen zu einem Bericht* auf Seite 277
  Sie können neue Elemente zu einem vorhandenen Bericht hinzufügen.
- *Konfigurieren von Bildelementen in Berichten* auf Seite 278
  Sie können neue Bilder hochladen und die in einem Bericht verwendeten Bilder ändern.
- *Konfigurieren von Textelementen in Berichten* auf Seite 278
  Sie können statischen Text in einen Bericht einfügen, um bestimmte Inhalte näher zu erklären.
- *Konfigurieren von Abfragetabellenelementen in Berichten* auf Seite 279
  Einige Abfragen sollten in Berichten in Tabellenform dargestellt werden.
- *Konfigurieren von Abfragediagrammelementen in Berichten* auf Seite 279
  Einige Abfragen sollten in Berichten in Diagrammform dargestellt werden.
- *Anpassen von Kopf- und Fußzeilen in Berichten* auf Seite 280
  Kopf- und Fußzeilen enthalten Informationen zu dem Bericht.
- *Entfernen von Elementen aus einem Bericht* auf Seite 281
  Wenn Elemente in einem Bericht nicht mehr benötigt werden, können Sie diese entfernen.
- *Ändern der Reihenfolge von Elementen in einem Bericht* auf Seite 281
  Sie können die Reihenfolge ändern, in der Elemente in einem Bericht angezeigt werden.

Hinzufügen von Elementen zu einem Bericht

Sie können neue Elemente zu einem vorhandenen Bericht hinzufügen.

> **Bevor Sie beginnen**
> Um diese Aktion durchführen zu können, muss ein Bericht auf der Seite **Bericht-Layout** geöffnet sein.

Vorgehensweise

Definitionen zu Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

1. Wählen Sie in der **Toolbox** ein Element aus, und ziehen Sie es über das **Bericht-Layout**.
2. Legen Sie das Element dort an der gewünschten Stelle ab.

   Bei anderen Berichtelementen als dem **Seitenumbruch** ist eine Konfiguration erforderlich. Die Konfigurationsseite für das Element wird angezeigt.
3. Klicken Sie nach Abschluss der Konfiguration des Elements auf **OK**.

Konfigurieren von Bildelementen in Berichten

Sie können neue Bilder hochladen und die in einem Bericht verwendeten Bilder ändern.

> **Bevor Sie beginnen**
> Es muss ein Bericht auf der Seite **Bericht-Layout** geöffnet sein.

Vorgehensweise

Definitionen zu Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

1. Zum Konfigurieren eines bereits in einem Bericht vorhandenen Bildes klicken Sie auf den Pfeil in der linken oberen Ecke des Bildes. Klicken Sie auf **Konfigurieren**.

   Dadurch wird die Seite **Konfigurieren: Text** angezeigt. Wenn Sie ein Bild zum Bericht hinzufügen, wird die Seite **Konfigurieren: Bild** angezeigt, nachdem Sie das **Bild**-Element auf dem Bericht abgelegt haben.
2. Wenn Sie ein vorhandenes Bild verwenden möchten, wählen Sie es in der Galerie aus.
3. Wenn Sie ein neues Bild verwenden möchten, klicken Sie auf **Durchsuchen**, und wählen Sie das Bild auf Ihrem Computer aus. Klicken Sie auf **OK**.
4. Wenn Sie eine bestimmte Bildbreite angeben möchten, geben Sie den Wert in das Feld **Bildbreite** ein.

   In der Standardeinstellung wird das Bild ohne Größenänderung in seiner Originalbreite angezeigt, solange das Bild nicht breiter als die Seite ist. Falls das Bild breiter ist, wird es unter Beibehaltung des Seitenverhältnisses auf die verfügbare Breite verkleinert.
5. Legen Sie fest, ob das Bild links, rechts oder zentriert ausgerichtet werden soll.
6. Klicken Sie auf **OK**.

Konfigurieren von Textelementen in Berichten

Sie können statischen Text in einen Bericht einfügen, um bestimmte Inhalte näher zu erklären.

> **Bevor Sie beginnen**
> Es muss ein Bericht auf der Seite **Bericht-Layout** geöffnet sein.

Vorgehensweise

Definitionen zu Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

1. Zum Konfigurieren eines bereits in einem Bericht vorhandenen Textes klicken Sie auf den Pfeil in der linken oberen Ecke des Textelements. Klicken Sie auf **Konfigurieren**.

   Dadurch wird die Seite **Konfigurieren: Text** angezeigt. Wenn Sie einen neuen Text zum Bericht hinzufügen, wird die Seite **Konfigurieren: Text** angezeigt, nachdem Sie das **Text**-Element auf dem Bericht abgelegt haben.

2. Sie können den vorhandenen Text im Bearbeitungsfeld **Text** bearbeiten oder neuen Text hinzufügen.

3. Bei Bedarf können Sie die Schriftgröße ändern.

   Der Standardwert ist Schriftgröße 12.

4. Wählen Sie die Textausrichtung aus: **Links**, **Zentriert** oder **Rechts**.

5. Klicken Sie auf **OK**.

Der von Ihnen eingegebene Text wird im Bericht-Layout innerhalb des Textelementes angezeigt.

Konfigurieren von Abfragetabellenelementen in Berichten

Einige Abfragen sollten in Berichten in Tabellenform dargestellt werden.

> **Bevor Sie beginnen**
> Es muss ein Bericht auf der Seite **Bericht-Layout** geöffnet sein.

Vorgehensweise

Definitionen zu Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

1. Zum Konfigurieren einer bereits in einem Bericht vorhandenen Tabelle klicken Sie auf den Pfeil in der linken oberen Ecke der Tabelle. Klicken Sie auf **Konfigurieren**.

   Dadurch wird die Seite **Konfigurieren: Abfragetabelle** angezeigt. Wenn Sie eine Abfragetabelle zum Bericht hinzufügen, wird die Seite **Konfigurieren: Abfragetabelle** angezeigt, nachdem Sie das **Abfragetabellen**-Element auf dem Bericht abgelegt haben.

2. Wählen Sie in der Dropdown-Liste **Abfrage** eine Abfrage aus.

3. Wählen Sie in der Dropdown-Liste **Datenbank** die Datenbank aus, in der die Abfrage ausgeführt werden soll.

4. Wählen Sie die Schriftgröße aus, mit der die Tabellendaten angezeigt werden sollen.

   Der Standardwert ist Schriftgröße 8.

5. Klicken Sie auf **OK**.

Konfigurieren von Abfragediagrammelementen in Berichten

Einige Abfragen sollten in Berichten in Diagrammform dargestellt werden.

> **Bevor Sie beginnen**
> Es muss ein Bericht auf der Seite **Bericht-Layout** geöffnet sein.

Vorgehensweise

Definitionen zu Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

1. Zum Konfigurieren eines bereits in einem Bericht vorhandenen Diagramms klicken Sie auf den Pfeil in der linken oberen Ecke des Diagramms. Klicken Sie auf **Konfigurieren**.

   Dadurch wird die Seite **Konfigurieren: Abfragediagramm** angezeigt. Wenn Sie ein Abfragediagramm zum Bericht hinzufügen, wird die Seite **Konfigurieren: Abfragediagramm** angezeigt, nachdem Sie das **Abfragetabellen**-Element auf dem Bericht abgelegt haben.

2. Wählen Sie in der Dropdown-Liste **Abfrage** eine Abfrage aus.
3. Legen Sie fest, ob nur das Diagramm, nur die Legende oder beides angezeigt werden soll.
4. Wenn sowohl das Diagramm als auch die Legende angezeigt werden sollen, müssen Sie auswählen, wie die beiden Elemente zueinander positioniert werden sollen.
5. Wählen Sie die Schriftgröße für die Legende aus.

   Der Standardwert ist Schriftgröße 8.

6. Wählen Sie die Bildhöhe für das Diagramm in Pixeln aus.

   Der Standardwert beträgt ein Drittel der Seitenhöhe.

7. Klicken Sie auf **OK**.

Anpassen von Kopf- und Fußzeilen in Berichten

Kopf- und Fußzeilen enthalten Informationen zu dem Bericht.

Innerhalb von Kopf- und Fußzeile gibt es sechs feste Positionen, an denen sich verschiedene Datenfelder befinden können. (Jeweils drei Positionen in der Kopfzeile und in der Fußzeile.)

Die Kopfzeile enthält ein links ausgerichtetes Logo und zwei übereinander angeordnete, rechts ausgerichtete Felder. Diese Felder können einen der vier folgenden Werte enthalten:

- Nichts
- Datum/Uhrzeit
- Seitennummer
- Benutzername des Benutzers, der den Bericht ausführt

Die Fußzeile verfügt ebenfalls über drei Felder: ein links ausgerichtetes, ein zentriertes ein rechts ausgerichtetes Feld. Diese drei Felder können einen der oben aufgeführten Werte oder auch benutzerdefinierten Text enthalten.

Vorgehensweise

Definitionen zu Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

1. Klicken Sie auf **Menü** | **Berichterstellung** | **Abfragen**. Wählen Sie die Registerkarte **Bericht** aus.
2. Wählen Sie einen Bericht aus, und klicken Sie auf **Aktionen** | **Bearbeiten**.
3. Klicken Sie auf **Kopf- und Fußzeile**.
4. In der Standardeinstellung verwenden Berichte bei Kopf- und Fußzeilen die Systemeinstellung. Wenn dies nicht gewünscht wird, deaktivieren Sie **Standard-Server-Einstellung verwenden**.

   Zum Ändern der Systemeinstellungen für Kopf- und Fußzeilen klicken Sie auf **Menü** | **Konfiguration** | **Server-Einstellungen**, wählen Sie dann **Drucken und exportieren** aus, und klicken Sie auf **Bearbeiten**.

5 Zum Ändern des Logos klicken Sie auf **Logo bearbeiten**.
   a Wenn als Logo ein Text angezeigt werden soll, wählen Sie **Text** aus, und geben Sie dann den Text in das Bearbeitungsfeld ein.
   b Zum Hochladen eines neuen Logos wählen Sie **Bild** aus, wechseln dann auf Ihrem Computer zu dem Bild und wählen es aus und klicken anschließend auf **OK**.
   c Wenn Sie ein bereits hochgeladenes Logo verwenden möchten, wählen Sie es aus.
   d Klicken Sie auf **Speichern**.
6 Ändern Sie die Kopf- und Fußzeile gemäß den gewünschten Daten, und klicken Sie dann auf **OK**.
7 Klicken Sie auf **Speichern**, um die am Bericht vorgenommenen Änderungen zu speichern.

Entfernen von Elementen aus einem Bericht

Wenn Elemente in einem Bericht nicht mehr benötigt werden, können Sie diese entfernen.

Vorgehensweise

Definitionen zu Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

1 Klicken Sie auf **Menü | Berichterstellung | Abfragen und Berichte**, und wählen Sie dann die Registerkarte **Bericht** aus.
2 Wählen Sie einen Bericht aus, und klicken Sie auf **Aktionen | Bearbeiten**.
3 Klicken Sie in der linken oberen Ecke des zu löschenden Elements auf den Pfeil und anschließend auf **Entfernen**.

   Das Element wird aus dem Bericht gelöscht.
4 Klicken Sie auf **Speichern**, um die am Bericht vorgenommenen Änderungen zu speichern.

Ändern der Reihenfolge von Elementen in einem Bericht

Sie können die Reihenfolge ändern, in der Elemente in einem Bericht angezeigt werden.

Vorgehensweise

Definitionen zu Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

1 Klicken Sie auf **Menü | Berichterstellung | Abfragen und Berichte**, und wählen Sie dann die Registerkarte **Bericht** aus.
2 Wählen Sie in der Liste einen Bericht aus, und klicken Sie auf **Aktionen | Bearbeiten**.
3 Klicken Sie zum Verschieben eines Elements auf dessen Titelleiste, und ziehen Sie es an eine neue Position.

   Die Elementpositionierung unter dem gezogenen Element ändert sich, während Sie den Cursor im Bericht bewegen. Wenn sich der Cursor über einer nicht zulässigen Position befindet, werden auf jeder Seite des Berichts rote Balken angezeigt.
4 Lassen Sie den Cursor los, wenn sich das Element an der gewünschten Position befindet.
5 Klicken Sie auf **Speichern**, um die am Bericht vorgenommenen Änderungen zu speichern.

Anzeigen von Berichtergebnissen

Sie können für jeden Bericht die zuletzt ausgeführte Version anzeigen.

Die Ergebnisse für einen Bericht werden bei jedem Ausführen auf dem Server gespeichert und in der Berichtsliste angezeigt.



Bei jedem Ausführen eines Berichts werden die vorherigen Ergebnisse gelöscht und können nicht mehr abgerufen werden. Wenn Sie die unterschiedlichen Durchläufe desselben Berichts vergleichen möchten, sollten Sie die Ergebnisse anderweitig archivieren.

Vorgehensweise

Definitionen zu Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

1. Klicken Sie auf **Menü** | **Berichterstellung** | **Abfragen und Berichte**, und wählen Sie dann die Registerkarte **Bericht** aus.
2. In der Berichtsliste sehen Sie eine Spalte **Ergebnis der letzten Ausführung**. Jeder Eintrag in dieser Spalte ist ein Link zu der PDF-Datei, die beim letzten erfolgreichen Ausführen des Berichts erstellt wurde. Klicken Sie zum Abrufen eines Berichts auf einen Link in dieser Spalte.

   Nun sollte eine PDF-Datei in Ihrem Browser geöffnet werden. Ihr Browser verhält sich dabei so, wie Sie es für diesen Dateityp konfiguriert haben.

Gruppieren von Berichten

Jeder Bericht muss einer Gruppe zugewiesen sein.

Berichte werden beim Erstellen einer Gruppe zugewiesen. Diese Zuweisung kann jedoch zu einem späteren Zeitpunkt geändert werden. Meist werden Berichte gruppiert, um ähnliche Berichte zusammenzufassen oder um Berechtigungen für bestimmte Berichte zu verwalten.

Vorgehensweise

Definitionen zu Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

1. Klicken Sie auf **Menü** | **Berichterstellung** | **Abfragen und Berichte**, und wählen Sie dann die Registerkarte **Bericht** aus.
2. Wählen Sie einen Bericht aus, und klicken Sie auf **Aktionen** | **Bearbeiten**.
3. Klicken Sie auf **Name, Beschreibung und Gruppe**.
4. Wählen Sie in der Dropdown-Liste **Berichtsgruppe** einen Bericht aus, und klicken Sie auf **OK**.
5. Klicken Sie auf **Speichern**, um am Bericht vorgenommene Änderungen zu speichern.

Wenn Sie die gewünschte Gruppe in der Liste **Gruppen** im linken Bereich des Berichtsfensters auswählen, wird der Bericht nun in der Berichtsliste angezeigt.

Ausführen von Berichten

Bevor Ergebnisse angezeigt werden können, müssen Berichte ausgeführt werden.

Berichte können in ePolicy Orchestrator in drei unterschiedlichen Speicherorten ausgeführt werden:

- In der Berichtsliste
- In einem Server-Task
- Auf der Seite **Bericht-Layout** beim Erstellen eines neuen oder Bearbeiten eines vorhandenen Berichts

Hier wird das Ausführen von Berichten in der Berichtsliste erläutert.

Vorgehensweise

Definitionen zu Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

1. Klicken Sie auf **Menü | Berichterstellung | Abfragen und Berichte**, und wählen Sie dann die Registerkarte **Bericht** aus.
2. Wählen Sie einen Bericht in der Berichtliste aus, und klicken Sie dann auf **Aktionen | Ausführen**.

   Nach Abschluss des Berichts wird die erstellte PDF an Ihren Browser gesendet. Je nach Ihren Browser-Einstellungen wird der Bericht entweder angezeigt oder heruntergeladen.

Die Berichterstellung kann mitunter einige Zeit dauern. Zwar können mehrere Berichte gleichzeitig ausgeführt, jedoch immer nur ein Bericht über die Benutzeroberfläche erstellt werden. Wenn der Bericht fertig gestellt ist, wird die Spalte **Ergebnis der letzten Ausführung** in der Berichtsliste mit einem Link zu der PDF-Datei aktualisiert, in der sich diese Ergebnisse befinden.

Ausführen eines Berichts mit einem Server-Task

Mithilfe von Server-Tasks können Berichte automatisch ausgeführt werden.

Wenn Sie einen Bericht ohne manuelles Eingreifen ausführen möchten, nutzen Sie am besten einen Server-Task. Mit der hier beschriebenen Vorgehensweise erstellen Sie einen neuen Server-Task, der automatische, geplante Ausführungen eines bestimmten Berichts ermöglicht.

Vorgehensweise

Definitionen zu Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

1. Klicken Sie auf **Menü | Automatisierung | Server-Tasks**, und klicken Sie dann auf **Aktionen | Neuer Task**.
2. Geben Sie für den Task einen geeigneten **Namen** und optional **Anmerkungen** ein. Legen Sie außerdem fest, ob der Task einen **Planungsstatus** besitzt. Klicken Sie auf **Weiter**.

   Wenn der Task automatisch ausgeführt werden soll, legen Sie den **Planungsstatus** auf **Aktiviert** fest.
3. Wählen Sie in der Dropdown-Liste **Aktionen** den Eintrag **Bericht ausführen** aus. Wählen Sie den auszuführenden Bericht sowie die Zielsprache aus. Klicken Sie auf **Weiter**.
4. Wählen Sie den **Planungstyp** (die Häufigkeit), das **Startdatum**, das **Enddatum** und die Uhrzeit aus, zu der der Bericht ausgeführt werden soll. Klicken Sie auf **Weiter**.

   Diese Planungsinformationen kommen nur zum Einsatz, wenn Sie die Option **Planungsstatus** aktivieren.
5. Klicken Sie auf **Speichern**, um den Server-Task zu speichern.

Der neue Task wird nun in der Liste **Server-Tasks** angezeigt.

Exportieren und Importieren von Berichten

Da Berichte mitunter sehr detaillierte Informationen enthalten, kann durch Exportieren und Importieren von einem Server auf einen anderen sichergestellt werden, dass der Datenabruf und die Berichterstellung auf allen ePolicy Orchestrator-Servern konsistent erfolgt.

Vorgehensweise

Definitionen zu Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

1. Öffnen Sie die Seite **Abfragen**, indem Sie **Menü | Berichterstellung | Abfragen und Berichte** und dann die Registerkarte **Bericht** auswählen.
2. Wählen Sie eine der folgenden Aktionen aus.

Aktion	Vorgehensweise
Exportieren von Berichten	1 Wählen Sie in der Liste **Gruppen** die Gruppe aus, in der sich die Berichte befinden, die Sie exportieren möchten. 2 Wählen Sie die Berichte aus, die Sie exportieren möchten, und klicken Sie dann auf **Aktionen | Exportieren**. Der McAfee ePO-Server sendet eine XML-Datei an Ihren Browser. Der nächste Schritt hängt von Ihren Browser-Einstellungen ab. Von den meisten Browsern werden Sie standardmäßig zum Speichern der Datei aufgefordert. Der exportierte Bericht enthält die Definitionen aller im Bericht enthaltenen Elemente. Dazu gehören u. a. externe Datenbankdefinitionen, Abfragen und Grafiken.
Importieren von Berichten	1 Klicken Sie auf der Seite **Bericht** auf **Aktionen | Importieren**. 2 Klicken Sie auf **Durchsuchen**, und wählen Sie die XML-Datei aus, in der sich der zu importierende Bericht befindet. 3 Wählen Sie eine neue oder eine vorhandene Gruppe für den Bericht aus. Wenn es sich um eine neue Gruppe handelt, geben Sie einen Namen für die Gruppe ein, und wählen Sie aus, ob sie privat oder öffentlich ist. Bei einer vorhandenen Gruppe wählen Sie die Gruppe für den importierten Bericht aus. 4 Klicken Sie auf **OK**. 5 Klicken Sie auf **Importieren**, um den Importvorgang abzuschließen. Den neu importierten Berichten werden die Berechtigungen der Gruppe zugewiesen, in die sie importiert wurden.

Konfigurieren der Vorlage und des Speicherorts für exportierte Berichte

Sie können das Erscheinungsbild und den Speicherort für Tabellen und Dashboards definieren, die Sie als Dokumente exportieren.

Mit der Server-Einstellung **Drucken und exportieren** können Sie Folgendes konfigurieren:

- Kopf- und Fußzeilen, einschließlich Name, Seitenzahl, eines benutzerdefinierten Logos usw.
- Seitengröße und -ausrichtung zum Drucken
- Das Verzeichnis, in dem exportierte Tabellen und Dashboards gespeichert werden

Vorgehensweise

Definitionen zu Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

1. Klicken Sie auf **Menü** | **Konfiguration** | **Server-Einstellungen**, und wählen Sie dann in der Liste **Einstellungskategorien** den Eintrag **Drucken und exportieren** aus.
2. Klicken Sie auf **Bearbeiten**. Die Seite **Drucken und exportieren: Bearbeiten** wird angezeigt.

3 Klicken Sie im Abschnitt **Kopf- und Fußzeilen für exportierte Dokumente** auf **Logo bearbeiten**, um die Seite **Logo bearbeiten** zu öffnen.

   a Wählen Sie **Text** aus, und geben Sie den Text ein, der in der Dokumentkopfzeile angezeigt werden soll, oder führen Sie einen der folgenden Schritte aus:

   - Wählen Sie **Bild** aus, und wechseln Sie zu der Bilddatei (z. B. zur Datei mit Ihrem Firmenlogo).
   - Wählen Sie das McAfee-Standardlogo aus.

   b Klicken Sie auf **OK**, um zur Seite **Drucken und exportieren: Bearbeiten** zurückzukehren.

4 Wählen Sie in den Dropdown-Listen die gewünschten Metadaten aus, die in der Kopf- und der Fußzeile angezeigt werden sollen.

5 Wählen Sie eine **Seitengröße** und eine **Seitenausrichtung** aus.

6 Geben Sie einen neuen Speicherort ein, oder übernehmen Sie den Standardspeicherort, in dem exportierte Dokumente gespeichert werden.

7 Klicken Sie auf **Speichern.**

Löschen von Berichten

Nicht mehr benötigte Berichte können gelöscht werden.

> **Bevor Sie beginnen**
> Zum Löschen eines Berichts müssen Sie Bearbeitungsberechtigungen für den Bericht besitzen.

Vorgehensweise

Definitionen zu Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

1 Klicken Sie auf **Menü** | **Berichterstellung** | **Abfragen und Berichte**, und wählen Sie dann die Registerkarte **Bericht** aus.

2 Wählen Sie in der Liste der Berichte einen oder mehrere Berichte zum Löschen aus.

3 Klicken Sie auf **Aktionen** | **Löschen**. Wenn Sie sicher sind, dass die Aktion durchgeführt werden soll, klicken Sie auf **Ja**.

Die Berichte wurden gelöscht. Server-Tasks, die auf gelöschte Berichte verweisen, sind nicht mehr gültig.

Konfigurieren von Internet Explorer 8 zum automatischen Akzeptieren von McAfee ePO-Downloads

Automatisch stattfindende Downloads von ePolicy Orchestrator können aus Sicherheitsgründen von Microsoft Internet Explorer blockiert werden. Dieses Verhalten können Sie durch eine Konfigurationsänderung in Internet Explorer ändern.

Bestimmte Vorgänge in ePolicy Orchestrator (wie das Ausführen eines Berichts oder das Exportieren von Informationen in eine XML-Datei) können dazu führen, dass Internet Explorer 8 Ihnen einen blockierten Download meldet.

Diese Information wird in Internet Explorer direkt unterhalb der Registerkartenleiste in einer gelben Leiste mit der folgenden Meldung angezeigt: `Der Download von Dateien von dieser Site auf den Computer wurde aus Sicherheitsgründen geblockt. Klicken Sie hier, um Optionen anzuzeigen`. Wenn Sie auf die Meldung klicken, erhalten Sie die Möglichkeit, die blockierte Datei

dieses eine Mal herunterzuladen. Diese Meldung wird jedoch jedes Mal angezeigt, wenn ePolicy Orchestrator versucht, Ihnen eine Datei zu senden. Wenn Sie möchten, dass diese Meldung grundsätzlich nicht mehr angezeigt wird, müssen Sie folgendermaßen vorgehen:

Vorgehensweise

1. Klicken Sie in Internet Explorer 8 auf **Extras | Internetoptionen**.
2. Wählen Sie die Registerkarte **Sicherheit** aus, und klicken Sie auf **Lokales Intranet**.

   Wenn Sie Ihren ePolicy Orchestrator-Server zu den vertrauenswürdigen Sites hinzugefügt haben, klicken Sie anstatt auf **Lokales Intranet** auf **Vertrauenswürdige Sites**.
3. Klicken Sie auf **Stufe anpassen**.
4. Führen Sie einen Bildlauf zur Option **Automatische Eingabeaufforderung für Dateidownloads** durch, und stellen Sie sie auf **Aktivieren** ein. Klicken Sie auf **OK** und dann zur Bestätigung auf **Ja**.
5. Klicken Sie auf **OK**, um das Dialogfeld **Internetoptionen** zu schließen.

Zukünftig kann die angeforderte Datei heruntergeladen werden, ohne dass die gelbe Warnleiste angezeigt wird.

Verwenden von Datenbank-Servern

ePolicy Orchestrator kann Daten nicht nur von eigenen Datenbanken abrufen, sondern auch von Erweiterungsdatenbanken.

Zum Durchführen von Tasks in ePolicy Orchestrator müssen Sie möglicherweise eine Reihe unterschiedlicher Server-Typen registrieren. Dazu können Authentifizierungs-Server, Active Directory-Kataloge, ePolicy Orchestrator-Server und Datenbank-Server gehören, die mit bestimmten von Ihnen installierten Erweiterungen zusammenarbeiten.

Datenbanktypen

Mit einer Erweiterung kann ein *Datenbanktyp* (der auch als "Schema" oder "Struktur" bezeichnet wird) bei ePolicy Orchestrator registriert werden. Anschließend kann diese Erweiterung Daten für Abfragen, Berichte, Dashboard-Monitore und Server-Tasks bereitstellen. Um diese Daten zu verwenden, müssen Sie den Server zunächst bei ePolicy Orchestrator registrieren.

Datenbank-Server

Ein *Datenbank-Server* ist eine Kombination aus einem Server und einem auf diesem Server installierten Datenbanktyp. Ein Server kann als Host für mehr als eine Datenbank dienen, und ein Datenbanktyp kann auf mehreren Servern installiert sein. Jede Kombination der beiden Komponenten muss separat registriert werden und wird als *Datenbank-Server* bezeichnet.

Nachdem Sie einen Datenbank-Server registriert haben, können Sie in Abfragen, Berichten, Dashboard-Monitoren und Server-Tasks Daten aus der Datenbank abrufen. Wenn mehrere Datenbanken mit dem gleichen Datenbanktyp registriert sind, müssen Sie eine der Datenbanken als Standardeinstellung für diesen Datenbanktyp auswählen.

Arbeiten mit Datenbank-Servern

Datenbank-Server können registriert, geändert, angezeigt und gelöscht werden.

Ändern einer Datenbankregistrierung

Wenn Verbindungs- oder Anmeldeinformationen für einen Datenbank-Server geändert werden, müssen Sie die Registrierung entsprechend anpassen.

Vorgehensweise

Definitionen zu Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

1. Öffnen Sie die Seite **Registrierte Server**, indem Sie **Menü** | **Konfiguration** | **Registrierte Server** auswählen.
2. Wählen Sie die zu bearbeitende Datenbank aus, und klicken Sie dann auf **Aktionen** | **Bearbeiten**.
3. Ändern Sie den Namen oder die Anmerkungen für den Server, und klicken Sie dann auf **Weiter**.
4. Ändern Sie die Informationen entsprechend. Wenn Sie die Datenbankverbindung überprüfen müssen, klicken Sie auf **Verbindung testen**.
5. Klicken Sie auf **Speichern**, um die Änderungen zu speichern.

Entfernen einer registrierten Datenbank

Wenn Datenbanken nicht mehr benötigt werden, können Sie sie aus dem System entfernen.

Vorgehensweise

Definitionen zu Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

1. Öffnen Sie die Seite **Registrierte Server**. Wählen Sie dazu **Menü** | **Konfiguration** | **Registrierte Server** aus.
2. Wählen Sie die zu löschende Datenbank aus, und klicken Sie auf **Aktionen** | **Löschen**.
3. Klicken Sie im angezeigten Bestätigungsdialogfeld auf **Ja**, um die Datenbank zu löschen.

Die Datenbank wurde gelöscht. Abfragen, Berichte oder andere Elemente in ePolicy Orchestrator, die die gelöschte Datenbank verwendet haben, werden als ungültig gekennzeichnet, bis sie einer anderen Datenbank zugeordnet werden.

20 Probleme und Tickets

Bei Problemen handelt es sich um Aktionselemente, die priorisiert, zugewiesen und nachverfolgt werden können.

Probleme

Benutzer können einfache Probleme manuell erstellen. Alternativ kann der McAfee ePO-Server als Reaktion auf Produktereignisse automatisch Probleme erstellen. Benutzer mit den entsprechenden Berechtigungen können ePolicy Orchestrator beispielsweise so konfigurieren, dass automatisch ein Problem des Typs "Benchmark-Regel-Compliance" erstellt wird, wenn während eines Audits ein nicht konformes System entdeckt wird.

Tickets

Ein Ticket ist die externe Entsprechung eines Problems, das in einem Ticket-Server vorhanden ist. Sobald einem Problem ein Ticket hinzugefügt wird, wird das Problem als "mit einem Ticket gekennzeichnetes Problem" bezeichnet. Einem mit einem Ticket gekennzeichneten Problem kann jedoch nur jeweils ein Ticket zugeordnet sein.

Integrieren von Problemen in Ticket-Server von Drittanbietern

Durch die Integration eines Ticket-Servers wird die Erstellung von Tickets erzwungen, die Problemen zugeordnet sind, die in Produkten erstellt wurden. ePolicy Orchestrator unterstützt die folgenden Ticket-Server:

- **Hewlett-Packard Openview Service Desk 4.5 und 5.1** – Eine integrierte Helpdesk- und Problem-Ticket-Lösung.
- **BMC Remedy Action Request System 6.3 und 7.0** – Eine konsolidierte Plattform zum Automatisieren und Verwalten von Problem-Tickets.

Inhalt

Beschreibung und Funktionsweise von Problemen

Die Art und Weise der Problemverwaltung wird von Benutzern mit den entsprechenden Berechtigungen und durch die installierten verwalteten Produkterweiterungen definiert.

Der Zustand, die Priorität, der Schweregrad, die Lösung, der Beauftragte und das Fälligkeitsdatum von Problemen werden von Benutzern definiert und können jederzeit geändert werden. Auf der Seite **Automatische Antworten** können Sie auch Standardantworten auf Probleme angeben. Diese Standardwerte werden basierend auf einer vom Benutzer konfigurierten Antwort automatisch angewendet, wenn ein Problem erstellt wird. Durch Antworten können auch mehrere Ereignisse in einem einzigen Problem aggregiert werden, sodass es zu keiner Überlastung des McAfee ePO-Servers mit zu vielen Problemen kommt.

Probleme können manuell gelöscht werden. Abgeschlossene Probleme können basierend auf ihrem Alter sowohl manuell als auch durch einen vom Benutzer konfigurierten Server-Task automatisch entfernt werden.

Arbeiten mit Problemen

Sie können Probleme erstellen, zuweisen, im Detail anzeigen, bearbeiten, löschen und bereinigen.

Aufgaben

- *Manuelles Erstellen von einfachen Problemen* auf Seite 290
  Einfache Probleme können manuell erstellt werden. Komplexere Probleme müssen automatisch erstellt werden.
- *Konfigurieren von Antworten zum automatischen Erstellen von Problemen* auf Seite 291
  Sie können Antworten verwenden, damit beim Eintreten bestimmter Ereignisse automatisch Probleme erstellt werden.
- *Verwalten von Problemen* auf Seite 292
  Sie können Probleme zuweisen, löschen, bearbeiten, ihre Details anzeigen und ihnen Anmerkungen hinzufügen.

Manuelles Erstellen von einfachen Problemen

Einfache Probleme können manuell erstellt werden. Komplexere Probleme müssen automatisch erstellt werden.

Vorgehensweise

Definitionen zu Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

1. Klicken Sie auf **Menü** | **Automatisierung** | **Probleme**, und klicken Sie dann auf **Aktionen** | **Neues Problem**.
2. Wählen Sie im Dialogfeld **Neues Problem** in der Dropdown-Liste **Problem vom folgenden Typ erstellen** den Typ **Einfach** aus, und klicken Sie dann auf **OK**.
3. Konfigurieren Sie das neue Problem.

Option	Aktion
Name	Geben Sie einen eindeutigen Namen für das Problem ein.
Beschreibung	Geben Sie eine eindeutige Beschreibung des Problems ein.

Option	Aktion
Zustand	Weisen Sie dem Problem einen Zustand zu: • Unbekannt • Neu • Zugewiesen • Gelöst • Abgeschlossen
Priorität	Weisen Sie dem Problem eine Priorität zu: • Unbekannt • Am niedrigsten • Niedrig • Mittel • Hoch • Am höchsten
Schweregrad	Weisen Sie dem Problem einen Schweregrad zu: • Unbekannt • Am niedrigsten • Niedrig • Mittel • Hoch • Am höchsten
Lösung	Weisen Sie dem Problem eine Lösung zu. Die Problemlösung kann erneut zugewiesen werden, sobald das Problem verarbeitet wird: • Keine • Behoben • Entfällt • Kann nicht behoben werden
Beauftragter	Geben Sie den Benutzernamen der Person ein, der das Problem zugewiesen wurde, oder wählen Sie die Person aus, indem Sie auf die Schaltfläche zum Durchsuchen […] klicken.
Fälligkeitsdatum	Legen Sie fest, ob das Problem ein Fälligkeitsdatum aufweisen soll. Falls ja, weisen Sie ein Datum und eine Uhrzeit für die Fälligkeit des Problems zu. In der Vergangenheit liegende Fälligkeitsdaten sind nicht zulässig.

4 Klicken Sie auf **Speichern**.

Konfigurieren von Antworten zum automatischen Erstellen von Problemen

Sie können Antworten verwenden, damit beim Eintreten bestimmter Ereignisse automatisch Probleme erstellt werden.

Vorgehensweise

Definitionen zu Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

1 Klicken Sie auf **Menü** | **Automatisierung** | **Automatische Antworten**, klicken Sie dann auf **Aktionen**, und wählen Sie **Neue Antwort** aus.

   Die Seite **Beschreibung** des **Antwort-Generators** wird angezeigt.

2 Füllen Sie die Felder aus, und klicken Sie dann auf **Weiter**.

3 Wählen Sie Eigenschaften aus, um die Ereignisse einzugrenzen, bei denen diese Antwort ausgelöst wird, und klicken Sie dann auf **Weiter**.

4. Wählen Sie neben **Aggregation** aus, wie häufig Ereignisse eintreten sollen, damit eine Antwort generiert wird.
5. Wählen Sie aus, nach welcher Methode Ereignisse gruppiert werden sollen.
6. Wählen Sie neben **Beschränkung** die maximale Zeitspanne aus, für die diese Antwort erfolgen soll.
7. Klicken Sie auf **Weiter**.
8. Wählen Sie **Problem erstellen** in der Dropdown-Liste aus, und wählen Sie dann den Typ für das zu erstellende Problem aus.

   Diese Auswahl bestimmt die Optionen, die auf dieser Seite angezeigt werden.
9. Geben Sie einen Namen und eine Beschreibung für das Problem ein. Wählen Sie bei Bedarf eine oder mehrere Variablen für den Namen und die Beschreibung aus.

   Diese Funktion stellt eine Reihe von Variablen bereit, die Informationen enthalten, die bei der Behebung des Problems hilfreich sein können.
10. Geben Sie gegebenenfalls weitere Optionen für die Antwort ein, oder wählen Sie sie aus.
11. Klicken Sie auf **Weiter**.
12. Überprüfen Sie die Einzelheiten zur Konfiguration der Antwort, und klicken Sie dann auf **Speichern**.

Verwalten von Problemen

Sie können Probleme zuweisen, löschen, bearbeiten, ihre Details anzeigen und ihnen Anmerkungen hinzufügen.

Vorgehensweise

Definitionen zu Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

1. Klicken Sie auf **Menü | Automatisierung | Probleme**.
2. Führen Sie die gewünschten Schritte aus.

Aktion	Vorgehensweise
Hinzufügen von Kommentaren zu Problemen	1 Aktivieren Sie das Kontrollkästchen neben jedem Problem, das Sie kommentieren möchten, und klicken Sie dann auf **Aktionen | Kommentar hinzufügen**. 2 Geben Sie im Bereich **Kommentar hinzufügen** den Kommentar ein, der zu den ausgewählten Problemen hinzugefügt werden soll. 3 Klicken Sie auf **OK**, um den Kommentar hinzuzufügen.
Hinzufügen von Tickets zu Problemen	Aktivieren Sie das Kontrollkästchen neben jedem Problem, dem Sie ein Ticket hinzufügen möchten, und klicken Sie dann auf **Aktionen | Ticket hinzufügen**.
Zuweisen von Problemen	Aktivieren Sie das Kontrollkästchen neben jedem Problem, das Sie zuweisen möchten, und klicken Sie dann auf **Einem Benutzer zuweisen**.
Anzeigen erforderlicher Spalten auf der Seite **Probleme**	Klicken Sie auf **Aktionen | Spalten auswählen**. Hier können Sie die Spalten mit Daten auswählen, die auf der Seite **Probleme** angezeigt werden sollen.

Aktion	Vorgehensweise
Löschen von Problemen	1 Aktivieren Sie das Kontrollkästchen neben jedem Problem, das Sie löschen möchten, und klicken Sie dann auf **Löschen**. 2 Klicken Sie im Bereich **Aktion** auf **OK**, um die ausgewählten Probleme zu löschen.
Bearbeiten von Problemen	1 Aktivieren Sie das Kontrollkästchen neben einem Problem, und klicken Sie dann auf **Bearbeiten**. 2 Nehmen Sie die gewünschten Änderungen am Problem vor. 3 Klicken Sie auf **Speichern**. Durch die Bearbeitung eines Problems wird die Problem/Ticket-Verbindung unterbrochen.
Exportieren der Liste von Problemen	Klicken Sie auf **Aktionen | Tabelle exportieren**. Die Seite **Exportieren** wird geöffnet. Auf der Seite **Exportieren** können Sie das Format der zu exportierenden Dateien, die Art, wie sie gepackt sind (z. B. in einer ZIP-Datei) und die weitere Vorgehensweise (z. B. per E-Mail als Anhang versenden) angeben.
Anzeigen von Problemdetails	Klicken Sie auf ein Problem. Die Seite **Problem: Details** wird angezeigt. Auf dieser Seite werden alle Einstellungen für das Problem sowie das Problemaktivitätsprotokoll angezeigt.

Bereinigen abgeschlossener Probleme

Sie können abgeschlossene Probleme in der Datenbank bereinigen, um sie dauerhaft zu löschen.

Durch das Bereinigen eines abgeschlossenen, mit einem Ticket gekennzeichneten Problems wird zwar das Problem gelöscht, das zugeordnete Ticket bleibt jedoch in der Datenbank des Ticket-Servers gespeichert.

Aufgaben

- *Manuelles Bereinigen abgeschlossener Probleme* auf Seite 293
  Durch regelmäßiges Bereinigen abgeschlossener Probleme in der Datenbank wird diese nicht zu voll.
- *Planmäßiges Bereinigen abgeschlossener Probleme* auf Seite 294
  Sie können einen Task planen, mit dem Sie abgeschlossene Probleme regelmäßig in der Datenbank bereinigen. Dadurch wird die Größe der Datenbank reduziert.

Manuelles Bereinigen abgeschlossener Probleme

Durch regelmäßiges Bereinigen abgeschlossener Probleme in der Datenbank wird diese nicht zu voll.

Vorgehensweise

Definitionen zu Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

1. Klicken Sie auf **Menü** | **Automatisierung** | **Probleme**, und klicken Sie dann auf **Aktionen** | **Bereinigen**.
2. Geben Sie im Dialogfeld **Bereinigen** eine Zahl ein, und wählen Sie dann eine Zeiteinheit aus.
3. Klicken Sie auf **OK**, um abgeschlossene Probleme zu bereinigen, die älter als das angegebene Datum sind.



Diese Funktion wirkt sich nicht nur auf die abgeschlossenen Probleme in der aktuellen Ansicht sondern auf alle abgeschlossenen Probleme aus.

Planmäßiges Bereinigen abgeschlossener Probleme

Sie können einen Task planen, mit dem Sie abgeschlossene Probleme regelmäßig in der Datenbank bereinigen. Dadurch wird die Größe der Datenbank reduziert.

Vorgehensweise

Definitionen zu Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

1. Klicken Sie auf **Menü** | **Automatisierung** | **Server-Tasks**, und klicken Sie dann auf **Aktionen** | **Neuer Task**.
2. Geben Sie einen Namen und eine Beschreibung für den Server-Task ein.
3. Aktivieren oder deaktivieren Sie den Plan für den Server-Task.

   Der Server-Task wird erst ausgeführt, nachdem er aktiviert wurde.
4. Klicken Sie auf **Weiter**.

   Daraufhin wird die Seite **Aktionen** angezeigt.
5. Wählen Sie in der Dropdown-Liste die Option **Abgeschlossene Probleme bereinigen** aus.
6. Geben Sie eine Zahl ein, und wählen Sie dann eine Zeiteinheit aus.
7. Klicken Sie auf **Weiter**.
8. Planen Sie den Server-Task, und klicken Sie dann auf **Weiter**.
9. Überprüfen Sie die Einzelheiten zur Konfiguration des Server-Tasks, und klicken Sie dann auf **Speichern**.

Die abgeschlossenen Probleme werden zum Zeitpunkt des geplanten Tasks bereinigt.

Beschreibung und Funktionsweise von Tickets

Ein Ticket ist die externe Entsprechung eines Problems, das in einem Ticket-Server vorhanden ist. Sobald einem Problem ein Ticket hinzugefügt wird, wird das Problem als "mit einem Ticket gekennzeichnetes Problem" bezeichnet.

Hinzufügen von Tickets zu Problemen

Tickets können manuell oder automatisch zu Problemen hinzugefügt werden. Einem mit einem Ticket gekennzeichneten Problem kann jedoch nur jeweils ein Ticket zugeordnet sein.

Wenn ein Ticket zu einem Problem hinzugefügt wird, ändert sich der Zustand des resultierenden, mit einem Ticket gekennzeichneten Problems in "Mit einem Ticket gekennzeichnet". Der Zustand des Problems vor der Kennzeichnung mit einem Ticket spielt dabei keine Rolle. Bei der Erstellung des Tickets im Ticket-Server wird die Ticket-ID zum mit einem Ticket gekennzeichneten Problem hinzugefügt. Die Ticket-ID stellt die Ticket/Problem-Zuordnung her.

Nachdem die Schritte zur Integration eines Ticket-Servers durchgeführt wurden, werden alle nachfolgenden Probleme automatisch mit einem Ticket gekennzeichnet. Es wird empfohlen, vor der Erstellung eines Tickets grundsätzlich einen Beauftragten zu einem Problem hinzuzufügen. Wenn ein Beauftragter manuell zu einem mit einem Ticket gekennzeichneten Problem hinzugefügt wird, müssen Sie Tickets zu allen Problemen, die vor der Integration bestanden, manuell hinzufügen.

Zuweisen von mit einem Ticket gekennzeichneten Problemen an Benutzer

Das manuelle Hinzufügen eines Beauftragten zu einem mit einem Ticket gekennzeichneten Problem wird als eine Bearbeitung des Problems betrachtet, durch die die Problem/Ticket-Zuordnung unterbrochen wird. Geben Sie für diesen Vorgang in der Antwort einen Beauftragten an, der Probleme erstellt. Auf diese Weise wird beim Erstellen des Problems automatisch ein Beauftragter zum Problem hinzugefügt.

Weitere Informationen finden Sie unter *Abschließen von Tickets und mit einem Ticket gekennzeichneten Problemen*.

Abschließen von Tickets und mit einem Ticket gekennzeichneten Problemen

Mit einem Ticket gekennzeichnete Probleme werden automatisch vom System abgeschlossen, wenn der Server-Task zur Synchronisierung von mit einem Ticket gekennzeichneten Problemen ausgeführt wird. Dieser Server-Task identifiziert Tickets, deren Zustand sich seit der letzten Ausführung des Tasks in "Abgeschlossen" geändert hat. Der Status eines mit einem Ticket gekennzeichneten und einem abgeschlossenen Ticket zugeordneten Problems wird dann in "Abgeschlossen" geändert. Darüber hinaus ersetzen die Kommentare im Ticket die Kommentare im mit einem Ticket gekennzeichneten Problem, falls die Ticket-Server-Integration so konfiguriert wurde, dass Kommentare in mit einem Ticket gekennzeichneten Problemen überschrieben werden.

Weitere Informationen finden Sie unter *Vorteile beim Hinzufügen von Kommentaren zu mit einem Ticket gekennzeichneten Problemen*.

Vorteile beim Hinzufügen von Kommentaren zu mit einem Ticket gekennzeichneten Problemen

Wenn Sie einen Kommentar zu einem mit einem Ticket gekennzeichneten Problem hinzufügen, wird dieser entweder sofort oder bei der nächsten Ausführung des Server-Tasks "Problemsynchronisierung" zum zugeordneten Ticket hinzugefügt. Kommentare in mit einem Ticket gekennzeichneten Problemen werden nur zu Tickets hinzugefügt, deren Zustand nicht "Abgeschlossen" lautet.

Wenn sich der Zustand des Tickets in "Abgeschlossen" ändert und der Ticket-Server zulässt, dass Problemkommentare durch Ticket-Kommentare überschrieben werden, ersetzen Kommentare für dieses Ticket sämtliche Kommentare im zugehörigen, mit einem Ticket gekennzeichneten Problem. Dieser Vorgang findet statt, wenn der Server-Task zur Synchronisierung von mit einem Ticket gekennzeichneten Problemen ein Ticket identifiziert, dessen Zustand sich nach der letzten Ausführung des Tasks in "Abgeschlossen" geändert hat. Für jedes abgeschlossene Ticket wird dieser Task nur ein

Mal durchgeführt. Wenn das Überschreiben von Problemkommentaren durch Ticket-Kommentare zugelassen wird, können Benutzer mit Zugriff auf das System (jedoch nicht auf den Ticket-Server) anzeigen, welche Änderungen am Ticket vorgenommen wurden.

Erneutes Öffnen von Tickets

Ein Ticket wird erneut geöffnet, wenn es zu einem zuvor hinzugefügten, mit einem Ticket gekennzeichneten Problem hinzugefügt wird, dessen ID mit einem Ticket im Ticket-Server abgeglichen werden kann. Falls die ID nicht abgeglichen werden kann, wird ein neues Ticket erstellt. Das erneute Öffnen eines Tickets führt nicht dazu, dass das zugeordnete, mit einem Ticket gekennzeichnete Problem ebenfalls erneut geöffnet wird.

Die Konfigurationszuordnung für den Ticket-Server muss ebenfalls konfiguriert werden, damit Tickets erneut geöffnet werden können. Weitere Informationen finden Sie unter *Erforderliche Felder für Zuordnungen*.

Synchronisierung von mit einem Ticket gekennzeichneten Problemen

Die Funktion **Probleme** umfasst den Server-Task "Problemsynchronisierung", der mit einem Ticket gekennzeichnete Probleme mit den zugeordneten Tickets im Ticket-Server synchronisiert. Dieser Server-Task ist standardmäßig deaktiviert und wird erst ausgeführt, nachdem er aktiviert wurde.

Bei der Ausführung des Server-Tasks versucht das System Folgendes:

- Ändern des Status der mit einem Ticket gekennzeichneten Probleme von **Mit einem Ticket gekennzeichnet** in **Abgeschlossen**, wenn der Zustand der zugeordneten Tickets **Abgeschlossen** lautet.
- Erstellen von Tickets für Probleme und Hinzufügen von Kommentaren zu Tickets, die das System zu einem früheren Zeitpunkt nicht erstellen oder hinzufügen konnte. Dies ist zum Beispiel der Fall, wenn beim ersten Hinzufügen der Tickets oder Kommentare ein Kommunikationsfehler aufgetreten ist.
- Ersetzen der Kommentare eines mit einem Ticket gekennzeichneten Problems durch die Kommentare des zugeordneten Tickets, wenn der Zustand des Tickets **Abgeschlossen** lautet und die Integration des Ticket-Servers so konfiguriert wurde, dass Kommentare von mit einem Ticket gekennzeichneten Problemen überschrieben werden.
- Ändern des Zustands jedes mit einem Ticket gekennzeichneten Problems in **Zugewiesen**, wenn für das mit einem Ticket gekennzeichnete Problem kein Beauftragter angegeben ist, oder in **Neu**, wenn der registrierte Server für den Ticket-Server gelöscht wird.

Integration in Ticket-Server

Durch die Integration eines Ticket-Servers wird die Erstellung von Tickets erzwungen, die Problemen zugeordnet sind, die in Produkten erstellt wurden.

ePolicy Orchestrator unterstützt die folgenden Ticket-Server:

- **Hewlett-Packard Openview Service Desk 4.5 und 5.1** – Eine integrierte Helpdesk- und Problem-Ticket-Lösung.
- **BMC Remedy Action Request System 6.3 und 7.0** – Eine konsolidierte Plattform zum Automatisieren und Verwalten von Problem-Tickets.

Die mit dieser Integration betraute Person sollte mit dem Ticket-Server sowie mit seinen Feldern und Formaten vertraut sein. Die Integration eines Ticket-Servers umfasst die folgenden grundlegenden Schritte:

1. Konfigurieren von ePolicy Orchestrator für die Integration in den Ticket-Server.



Das System, auf dem die Ticket-Erweiterung ausgeführt wird, muss die Adresse des Hewlett-Packard Openview Service Desk-Systems auflösen können. Hierzu zählt möglicherweise, dass die IP-Adresse des Service Desk-Systems zur Hostdatei auf dem System hinzugefügt wird, auf dem die Ticket-Erweiterung ausgeführt wird, oder dass eine Domänenvertrauensstellung zwischen den beiden Systemen eingerichtet wird. Weitere Informationen finden Sie unter *Konfigurieren des DNS für Hewlett-Packard Openview Service Desk 4.5*.

2. Integrieren eines Ticket-Servers in ePolicy Orchestrator. Es kann nur ein registrierter Ticket-Server in ePolicy Orchestrator integriert werden.
3. Konfigurieren der Feldzuordnungen zwischen Problemen und Tickets.

Erwägungen beim Löschen eines registrierten Ticket-Servers

In bestimmten Situationen möchten Sie eventuell den registrierten Server für den Ticket-Server löschen. Dies kann beispielsweise bei einer Aktualisierung des Ticket-Servers der Fall sein.

Wenn der registrierte Server gelöscht wird, ändert das System bei der nächsten Ausführung des Server-Tasks "Problemsynchronisierung" den Zustand jedes mit einem Ticket gekennzeichneten Problems in "Zugewiesen" beziehungsweise in "Neu", falls für das mit einem Ticket gekennzeichnete Problem kein Beauftragter angegeben ist. Aus diesem Grund ist es wichtig, bei einer Aktualisierung des Ticket-Servers die Planung für diesen Server-Task zu deaktivieren. Weitere Informationen finden Sie unter *Aktualisieren eines registrierten Ticket-Servers*.

Wenn der registrierte Ticket-Server gelöscht wird, bleibt die Ticket-ID, durch die das Ticket mit dem entsprechenden Problem verknüpft wurde, diesem mit einem Ticket gekennzeichneten Problem zugeordnet. Dadurch kann das Ticket erneut geöffnet werden, falls die Problem/Ticket-Zuordnung unterbrochen wird. Zum Beispiel, wenn der Server-Task ausgeführt wird, bevor der aktualisierte Server registriert ist. Weitere Informationen dazu finden Sie unter *Erneutes Öffnen von Tickets*.

Erforderliche Felder für Zuordnungen

Bei einer Zuordnung handelt es sich um den Vorgang, durch den Informationen in Problemen zu Informationen in Tickets zugeordnet werden. Jedes einzelne Informationselement wird als Feld bezeichnet. Die Felder in Problemen müssen entsprechenden Feldern in Tickets zugeordnet werden.

Um zu bestimmen, welche Ticket-Felder zugeordnet werden müssen, überprüfen Sie die Felder, die für die Erstellung eines Tickets im Ticket-Format des Ticket-Servers erforderlich sind. In der Dokumentation zum Ticket-Server finden Sie Informationen dazu, welche Felder ausgefüllt werden müssen.

Damit das System feststellen kann, wann mit einem Ticket gekennzeichnete Probleme abgeschlossen werden sollen, muss das Feld mit dem Zustand des Tickets zugeordnet werden.

Beispielzuordnungen

Bei der Registrierung des Ticket-Servers müssen Sie auch die Feldzuordnungen für Probleme und Tickets konfigurieren.



Die Feldzuordnungen in den folgenden Beispielen dienen nur zu Referenzzwecken. Ihre eigenen Zuordnungen sind abhängig von den im Ticket-Server erforderlichen Feldern und den Werten, die in diese Felder eingegeben werden können.

Bei einer Zuordnung handelt es sich um einen wechselseitigen Vorgang. Diese Beispiele veranschaulichen, wie ein Problem einem Ticket zugeordnet wird und wie der Ticket-Status wiederum dem Problemstatus zugeordnet wird. Ist das Ticket beispielsweise als abgeschlossen gekennzeichnet, wird der Problemstatus ebenfalls entsprechend aktualisiert.

Beispielzuordnung für Hewlett-Packard Openview Service Desk

Diese Beispielzuordnung für Hewlett-Packard Openview Service Desk 4.5 und 5.1 dient nur zu Referenzzwecken.



Quellwerte, zugeordnete Werte und Feld-IDs berücksichtigen Groß- und Kleinschreibung.

Problem zu folgendem Ticket zuordnen

- **Ticket-Format**: Standard_Problem
- **Ticket-Feld**: Beschreibung
  - **Vorgang**: Identität
  - **Quellfeld**: Name
- **Ticket-Feld**: Status
  - **Vorgang**: Ersatz
  - **Quellfeld**: Zustand
  - **Werte**: **Standardwert**: 10

Quellwert	Zugeordneter Wert
NEU	10
GELÖST	20
UNBEKANNT	20
ZUGEWIESEN	20

- **Ticket-Feld**: Information
  - **Vorgang**: Identität
  - **Quellfeld**: Beschreibung
- **Ticket-Feld**: HistoryLines
  - **Vorgang**: Identität
  - **Quellfeld**: Aktivitätsprotokoll
- **Ticket-Feld**: Geben Sie den Namen oder die ID für alle offenen Textfelder ein.
  - **Vorgang**: Identität
  - **Quellfeld**: URL

Ticket zurück auf das Problemstatusfeld verweisen



Da dieser Bereich nur den Ticket-Status zuordnet, werden Sie nicht dazu aufgefordert, die ID zum Statusfeld des Problems hinzuzufügen. Dieses Feld ist impliziert.

- **Vorgang**: Ersatz
- **Quellfeld**: Status

- **Werte**: **Standardwert**: MIT EINEM TICKET GEKENNZEICHNET

Quellwert	Zugeordneter Wert
40	ABGESCHLOSSEN

- **Problemkommentare mit Ticket-Kommentaren überschreiben**: Ausgewählt
- **Ticket-Kommentarfeld**: HistoryLines
- **Tickets können erneut geöffnet werden**: Ausgewählt

Beispielzuordnung für BMC Remedy Action Request System

Diese Beispielzuordnung für BMC Remedy Action Request System 6.3 und 7.0 dient nur zu Referenzzwecken.



Quellwerte, zugeordnete Werte und Feld-IDs berücksichtigen Groß- und Kleinschreibung.

Problem zu folgendem Ticket zuordnen

- **Ticket-Format**: Helpdesk
- **Ticket-Feld**: 8
  - **Vorgang**: Identität
  - **Quellfeld**: Name
- **Ticket-Feld**: 7
  - **Vorgang**: Ersatz
  - **Quellfeld**: Zustand
  - **Werte**: **Standardwert**: 0

Quellwert	Zugeordneter Wert
NEU	0
GELÖST	2
ZUGEWIESEN	1

- **Ticket-Feld**: 2
  - **Vorgang**: Benutzerdefinierte Zuordnung
  - **Quellfeld**: Geben Sie den Benutzernamen für den Ticket-Server ein. Dies ist derselbe Benutzername, der im **Generator für registrierte Server** auf der Seite **Beschreibung** unter **Authentifizierung** angegeben ist.
- **Ticket-Feld**: 200000004
  - **Vorgang**: Benutzerdefinierte Zuordnung
  - **Quellfeld**: Extern



In diesem Beispiel gibt "Extern" an, dass das Ticket von einem für den Ticket-Server externen Produkt erstellt wurde. Sie können stattdessen den Namen des Produkts eingeben und so angeben, welches Produkt das Ticket erstellt hat.

- **Ticket-Feld**: 240000008



Ticket-Systeme können über mehrere Kommentar- oder Kalenderfelder verfügen. Vergewissern Sie sich, dass Sie das Feld auswählen, das für diese Integration verwendet werden soll. Falls ein Kommentarfeld nicht zugeordnet ist, können Kommentare zu einem mit einem Ticket gekennzeichneten Problem nicht zu Tickets hinzugefügt werden.

  - **Vorgang**: Identität
  - **Quellfeld**: Aktivitätsprotokoll
- **Ticket-Feld**: Geben Sie den Namen oder die ID für alle offenen Textfelder ein.
  - **Vorgang**: Identität
  - **Quellfeld**: URL

Ticket zurück auf das Problemstatusfeld verweisen



Da dieser Bereich nur den Ticket-Status zuordnet, werden Sie nicht dazu aufgefordert, die ID zum Statusfeld des Problems hinzuzufügen. Dieses Feld ist impliziert.

- **Vorgang**: Ersatz
- **Quellfeld**: 7
- **Werte**: **Standardwert**: 0

Quellwert	Zugeordneter Wert
4	ABGESCHLOSSEN

- **Problemkommentare mit Ticket-Kommentaren überschreiben**: Ausgewählt
- **Ticket-Kommentarfeld**: 240000008
- **Tickets können erneut geöffnet werden**: Ausgewählt

Arbeiten mit Tickets

Mit dem Server-Task "Problemsynchronisierung" können Sie Tickets zu Problemen hinzufügen und mit Tickets gekennzeichnete Probleme synchronisieren.

Aufgaben

- *Hinzufügen von Tickets zu Problemen* auf Seite 301
  Sie können ein Ticket zu einem einzelnen Problem hinzufügen bzw. in einem Schritt zu mehreren Problemen hinzufügen.
- *Synchronisieren von mit einem Ticket gekennzeichneten Problemen* auf Seite 301
  Mit dem Server-Task "Problemsynchronisierung" werden mit einem Ticket gekennzeichnete Probleme und die zugeordneten Tickets im Ticket-Server synchronisiert.
- *Planmäßiges Synchronisieren von mit einem Ticket gekennzeichneten Problemen* auf Seite 301
  Mit dem Server-Task "Problemsynchronisierung" werden mit einem Ticket gekennzeichnete Probleme und die zugeordneten Tickets im Ticket-Server synchronisiert. Gehen Sie wie in dieser Aufgabe beschrieben vor, um den Server-Task "Problemsynchronisierung" für eine planmäßige Ausführung zu konfigurieren.

Hinzufügen von Tickets zu Problemen

Sie können ein Ticket zu einem einzelnen Problem hinzufügen bzw. in einem Schritt zu mehreren Problemen hinzufügen.

In ähnlicher Form kann ein Ticket beim Anzeigen der Details eines Problems hinzugefügt werden. Beim Hinzufügen eines Tickets wird im Ticket-Server automatisch ein neues Ticket erstellt. Probleme mit bestehenden Tickets werden ignoriert.

Vorgehensweise

Definitionen zu Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

1. Klicken Sie auf **Menü** | **Automatisierung** | **Probleme**, aktivieren Sie die Kontrollkästchen neben den einzelnen Problemen, und klicken Sie dann auf **Aktionen** | **Ticket hinzufügen**.
2. Klicken Sie im Dialogfeld **Ticket hinzufügen** auf **OK**, um ein Ticket zu jedem ausgewählten Problem hinzuzufügen.

Synchronisieren von mit einem Ticket gekennzeichneten Problemen

Mit dem Server-Task "Problemsynchronisierung" werden mit einem Ticket gekennzeichnete Probleme und die zugeordneten Tickets im Ticket-Server synchronisiert.

Vorgehensweise

Definitionen zu Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

1. Klicken Sie auf **Menü** | **Automatisierung** | **Server-Tasks**.
2. Klicken Sie neben dem Task **Problemsynchronisierung** auf **Ausführen**.
3. Überprüfen Sie die Ergebnisse des Server-Tasks.

   Weitere Informationen finden Sie in diesem Handbuch im Abschnitt zum Server-Task-Protokoll.

Planmäßiges Synchronisieren von mit einem Ticket gekennzeichneten Problemen

Mit dem Server-Task "Problemsynchronisierung" werden mit einem Ticket gekennzeichnete Probleme und die zugeordneten Tickets im Ticket-Server synchronisiert. Gehen Sie wie in dieser Aufgabe beschrieben vor, um den Server-Task "Problemsynchronisierung" für eine planmäßige Ausführung zu konfigurieren.



Der Zeitplan für den Server-Task "Problemsynchronisierung" ist standardmäßig deaktiviert.

Vorgehensweise

Definitionen zu Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

1. Klicken Sie auf **Menü** | **Automatisierung** | **Server-Tasks**, und klicken Sie dann in der Spalte **Aktionen** für den Task **Problemsynchronisierung** auf **Bearbeiten**.
2. Klicken Sie neben **Planungsstatus** auf **Aktiviert**.

   Wenn Sie den Zeitplan deaktivieren, wird der Server-Task nicht planmäßig ausgeführt. Sie können ihn aber weiterhin manuell ausführen.
3. Klicken Sie auf **Weiter**.
4. Klicken Sie auf der Registerkarte **Aktionen** auf **Weiter**.

5 Planen Sie den Server-Task nach Bedarf, und klicken Sie dann auf **Weiter**.

6 Überprüfen Sie die Einzelheiten zur Konfiguration des Server-Tasks, und klicken Sie dann auf **Speichern**.

Arbeiten mit Ticket-Servern

Mit diesen Aufgaben werden Ticket-Server in ePolicy Orchestrator integriert.

Aufgaben

- *Installieren von Erweiterungen für Ticket-Server* auf Seite 302
  Sie müssen das Ticket-System in ePolicy Orchestrator integrieren, bevor Sie Tickets erstellen können. Welche Dateien Sie dazu in ePolicy Orchestrator kopieren, hängt vom Ticket-System ab.
- *Registrieren und Zuordnen eines Ticket-Servers* auf Seite 305
  Gehen Sie wie in diesen Aufgaben beschrieben vor, um einen Ticket-Server zu registrieren und zuzuordnen. Sie müssen diese Schritte ausführen, bevor Tickets zu Problemen hinzugefügt werden können. Es kann nur jeweils ein registrierter Ticket-Server vorhanden sein.
- *Konfigurieren der Feldzuordnungen* auf Seite 306
  Bevor Sie Tickets zu Problemen zuordnen können, müssen Sie die Feldzuordnungen für einen Ticket-Server konfigurieren.

Installieren von Erweiterungen für Ticket-Server

Sie müssen das Ticket-System in ePolicy Orchestrator integrieren, bevor Sie Tickets erstellen können. Welche Dateien Sie dazu in ePolicy Orchestrator kopieren, hängt vom Ticket-System ab.

Vorgehensweise

1 Wechseln Sie zu **Start** | **Systemsteuerung** | **Verwaltung**, und doppelklicken Sie auf **Dienste**.

2 Doppelklicken Sie in der Spalte **Name** auf **McAfee ePolicy Orchestrator-Anwendungs-Server**.

3 Klicken Sie auf die Registerkarte **Allgemein**.

4 Klicken Sie unter **Dienststatus** auf **Stopp**.

Der Server wird nun angehalten.

5 Kopieren Sie die erforderlichen Dateien für Ihren Ticket-Server, und wiederholen Sie die Schritte 1 bis 3.

6 Klicken Sie unter **Dienststatus** auf **Start**.

Der Server wird nun ausgeführt.

Aufgaben

- *Anhalten und Starten des Servers* auf Seite 303
  Sie müssen den ePolicy Orchestrator-Server anhalten, bevor Sie die für den Ticket-Server erforderlichen Dateien kopieren können. Nachdem die Dateien kopiert wurden, starten Sie den Server erneut.
- *Kopieren der Hewlett-Packard Openview Service Desk-Dateien* auf Seite 303
  Bevor Sie die Hewlett-Packard Openview Service Desk (Service Desk) 5.1- oder 4.5-Erweiterung verwenden können, müssen Sie bestimmte Dateien kopieren. Weitere Informationen zu diesen Dateien finden Sie in der Dokumentation zu Service Desk.
- *Kopieren der BMC Remedy Action Request System-Dateien* auf Seite 303
  Bevor Sie die Erweiterung von BMC Remedy Action Request System (Remedy) verwenden können, müssen Sie bestimmte Dateien kopieren. Weitere Informationen zu diesen Dateien finden Sie in der Dokumentation zu Remedy. Die Remedy-Erweiterung bietet Unterstützung für Remedy 6.3- und Remedy 7.0-Server.
- *Installieren der Erweiterungen für Ticket-Server* auf Seite 304
  Bevor Sie die Ticket-Server-Erweiterungen in das ePolicy Orchestrator-Ticket-System integrieren können, müssen Sie sie installieren.

Anhalten und Starten des Servers

Sie müssen den ePolicy Orchestrator-Server anhalten, bevor Sie die für den Ticket-Server erforderlichen Dateien kopieren können. Nachdem die Dateien kopiert wurden, starten Sie den Server erneut.

Vorgehensweise

1. Klicken Sie in Windows auf **Start** | **Systemsteuerung** | **Verwaltung**, und doppelklicken Sie dann auf **Dienste**.
2. Suchen Sie in der Spalte **Name** den Eintrag **McAfee ePolicy Orchestrator-Anwendungs-Server**, und doppelklicken Sie darauf.
3. Klicken Sie auf die Registerkarte **Allgemein**.
4. Klicken Sie unter **Dienststatus** auf **Stopp**.

   Der Server wird nun angehalten.
5. Kopieren Sie die erforderlichen Dateien für Ihren Ticket-Server, und wiederholen Sie die Schritte 1 bis 3.
6. Klicken Sie unter **Dienststatus** auf **Start**.

   Der Server wird nun ausgeführt.

Kopieren der Hewlett-Packard Openview Service Desk-Dateien

Bevor Sie die Hewlett-Packard Openview Service Desk (Service Desk) 5.1- oder 4.5-Erweiterung verwenden können, müssen Sie bestimmte Dateien kopieren. Weitere Informationen zu diesen Dateien finden Sie in der Dokumentation zu Service Desk.

- Kopieren Sie die erforderlichen Dateien in den Ordner `\Server\common\lib` Ihrer ePolicy Orchestrator-Installation.

  Beispiel: `C:\Programme\McAfee\ePolicy Orchestrator\Server\common\lib`.

Kopieren der BMC Remedy Action Request System-Dateien

Bevor Sie die Erweiterung von BMC Remedy Action Request System (Remedy) verwenden können, müssen Sie bestimmte Dateien kopieren. Weitere Informationen zu diesen Dateien finden Sie in der

Dokumentation zu Remedy. Die Remedy-Erweiterung bietet Unterstützung für Remedy 6.3- und Remedy 7.0-Server.



Für die Remedy-Erweiterung können Sie die API-Dateien von Remedy 5.1 oder 7.0 verwenden. Eine Integration mit dem Remedy 5.1-Server wird von McAfee nicht unterstützt, die API-Dateien von Version 5.1 funktionieren jedoch bei Integrationen mit Remedy 6.3- oder 7.0-Servern. Die API-Dateien von Remedy 6.3 werden nicht unterstützt.

Vorgehensweise

1 Kopieren Sie die folgenden erforderlichen Dateien in den Ordner **\Server\bin** Ihrer ePolicy Orchestrator-Installation. Beispiel: `C:\Programme\McAfee\ePolicy Orchestrator\Server\bin`.

Remedy-API-Version	Erforderliche Dateien	
Remedy 5.1	• ARAPI51.DLL • ARJNI51.DLL • ARRPC51.DLL • ARUTL51.DLL	
Remedy 7.0	• ARAPI70.DLL • ARJNI70.DLL • ARRPC70.DLL • ARUTILJNI70.DLL • ARUTL70.DLL	• ARXMLUTIL70.DLL • ICUDT32.DLL • ICUIN32.DLL • ICUUC32.DLL

2 Kopieren Sie die folgenden erforderlichen Dateien in den Ordner **\Server\common\lib** Ihrer ePolicy Orchestrator-Installation. Beispiel: `C:\Programme\McAfee\ePolicy Orchestrator\Server\common\lib`.

Remedy-API-Version	Erforderliche Dateien
Remedy 5.1	• ARAPI51.JAR • ARUTIL51.JAR
Remedy 7.0	• ARAPI70.JAR • ARUTIL70.JAR

Installieren der Erweiterungen für Ticket-Server

Bevor Sie die Ticket-Server-Erweiterungen in das ePolicy Orchestrator-Ticket-System integrieren können, müssen Sie sie installieren.

Vorgehensweise

Definitionen zu Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

1 Klicken Sie auf **Menü** | **Software** | **Erweiterungen** und anschließend auf **Erweiterung installieren**.



> Das Master-Repository darf nicht durch mehrere Tasks gleichzeitig aktualisiert werden. Wenn Sie versuchen, während einer Aktualisierung des Master-Repositorys eine Erweiterung zu installieren, wird die folgende Fehlermeldung angezeigt:
>
> Die Erweiterung kann nicht installiert werden. com.mcafee.core.cdm.CommandException: Das ausgewählte Paket kann während eines Abruf-Tasks nicht eingecheckt werden.
>
> Warten Sie, bis die Aktualisierung des Master-Repositorys abgeschlossen ist, und versuchen Sie dann erneut, die Erweiterung zu installieren.

2 Wechseln Sie in den Ordner `<Installationsverzeichnis>\ePolicy Orchestrator\Installer\Core\Extensions`, und wählen Sie die gewünschte Erweiterungsdatei (ZIP) aus.

Erweiterungen für BMC Remedy 6.3 und 7.0 sowie Hewlett-Packard Openview Service Desk 4.5 und 5.1 sind in ePolicy Orchestrator enthalten.

3 Klicken Sie auf **OK**.

Registrieren und Zuordnen eines Ticket-Servers

Gehen Sie wie in diesen Aufgaben beschrieben vor, um einen Ticket-Server zu registrieren und zuzuordnen. Sie müssen diese Schritte ausführen, bevor Tickets zu Problemen hinzugefügt werden können. Es kann nur jeweils ein registrierter Ticket-Server vorhanden sein.

Aufgaben

- *Konfigurieren des DNS für Hewlett-Packard Openview Service Desk 4.5* auf Seite 305
  Bevor Sie eine Integration in Service Desk 4.5 durchführen können, müssen Sie die Server-Daten konfigurieren.
- *Registrieren eines Ticket-Servers* auf Seite 306
  Sie müssen einen Ticket-Server registrieren, bevor Tickets zu Problemen zugeordnet werden können.

Konfigurieren des DNS für Hewlett-Packard Openview Service Desk 4.5

Bevor Sie eine Integration in Service Desk 4.5 durchführen können, müssen Sie die Server-Daten konfigurieren.

Das System, auf dem die Ticket-Erweiterung ausgeführt wird, muss die Adresse des Service Desk-Systems auflösen können.

Vorgehensweise

1 Öffnen Sie auf dem in das Ticket-System integrierten McAfee ePO-Server mithilfe einer Textanweisung die Datei **hosts**.

Diese Datei befindet sich im Ordner `c:\Windows\system32\drivers\etc\`.

2 Bearbeiten Sie die Datei **hosts** so, dass sie die IP-Adresse des Systems enthält, auf dem Service Desk 4.5 ausgeführt wird, gefolgt von einem Leerzeichen, gefolgt vom DNS-Suffix (dem Namen des Systems, auf dem Service Desk 4.5 ausgeführt wird).

Beispiel: `168.212.226.204 SRVDSK45.qaad.com`

3 Speichern und schließen Sie die Datei **hosts**.

4 Starten Sie den McAfee ePO-Server neu.

Registrieren eines Ticket-Servers

Sie müssen einen Ticket-Server registrieren, bevor Tickets zu Problemen zugeordnet werden können.

Vorgehensweise

Definitionen zu Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

1. Klicken Sie auf **Menü** | **Konfiguration** | **Registrierte Server**, und klicken Sie dann auf **Neuer Server**.
2. Wählen Sie den Server-Typ für den Ticket-Server aus.

   Je nachdem, welchen Datentyp Sie ausgewählt haben, sind auf den nachfolgenden Seiten des Generators unterschiedliche Optionen verfügbar.
3. Geben Sie einen Namen und eine Beschreibung ein, und klicken Sie dann auf **Weiter**.
4. Geben Sie den Host für den Server ein.
5. Geben Sie den Port, den Benutzernamen und das Kennwort für den Server ein.
6. Wenn Service Desk 4.5 oder 5.1 ausgewählt wurde, wählen Sie einen **Workflow** aus.

Konfigurieren der Feldzuordnungen

Bevor Sie Tickets zu Problemen zuordnen können, müssen Sie die Feldzuordnungen für einen Ticket-Server konfigurieren.

Aufgaben

- *Zuordnen von Problemen zu Tickets* auf Seite 306
  Die Konfiguration der Feldzuordnung zwischen Problem und Ticket, sorgt dafür, dass die Daten bei Verwendung eines Ticket-Servers synchronisiert werden.
- *Zurückverweisen von Tickets auf den Problemstatus* auf Seite 307
  Sie müssen eine Feldzuordnung zwischen Ticket und Problem mit Rückverweis auf das Statusfeld (den Zustand) des Problems konfigurieren, um den Ticket-Server vollständig zu integrieren.

Zuordnen von Problemen zu Tickets

Die Konfiguration der Feldzuordnung zwischen Problem und Ticket, sorgt dafür, dass die Daten bei Verwendung eines Ticket-Servers synchronisiert werden.



Quellwerte, zugeordnete Werte und Feld-IDs berücksichtigen Groß- und Kleinschreibung.

Vorgehensweise

Definitionen zu Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

1. Klicken Sie neben **Zuordnung konfigurieren** auf **Konfigurieren**.
2. Wählen Sie im Bereich **Zuordnungsoptionen** nach Bedarf Optionen aus.

   Ausgewählte Optionen werden im Bereich **Zuordnungsdefinitionen** mit Operatoren angezeigt, die angeben, wie ein Problem einem Ticket zugeordnet werden soll und wie ein Ticket dann zurück auf ein Problem zu verweisen ist. Es müssen beide Zuordnungen vorgenommen werden.
3. Geben Sie unter **Problem zu folgendem Ticket zuordnen** den Namen eines **Ticket-Formats** ein.
4. Geben Sie unter **Ticket-Feld** eine ID ein.

5 Wählen Sie einen **Vorgang** aus.

6 Führen Sie eine der folgenden Aktionen aus:

- Falls **Ersatz** ausgewählt ist, wählen Sie in der Dropdown-Liste **Quellfeld** ein Problemfeld aus, und klicken Sie dann neben **Werte** auf **Bearbeiten**. Das Dialogfeld **Ersatzzuordnung bearbeiten** wird angezeigt.

  1 Geben Sie einen **Standardwert** ein, der ersetzt werden soll, wenn ein nicht zugeordneter Quellwert zurückgegeben wird.

  2 Geben Sie einen **Quellwert** für das Problem und anschließend unter **Zugeordneter Wert** den zugeordneten Wert ein, der durch diesen Wert im Ticket ersetzt werden soll.

  3 Klicken Sie auf **+**, um einen anderen Wert zuzuordnen.

  4 Klicken Sie abschließend auf **OK**.

- Falls **Wertebereich** ausgewählt ist, wählen Sie in der Dropdown-Liste **Quellfeld** ein zuzuordnendes Problemfeld aus, und klicken Sie dann neben **Werte** auf **Bearbeiten**. Das Dialogfeld **Numerische Bereichszuordnung bearbeiten** wird angezeigt.

  1 Geben Sie einen **Standardwert** ein, der ersetzt werden soll, wenn ein nicht zugeordneter Quellbereich zurückgegeben wird.

  2 Geben Sie den **Quellbereich** für das Problem und anschließend unter **Zugeordneter Wert** den zugeordneten Wert ein, der durch diesen Bereich im Ticket ersetzt werden soll.

  3 Klicken Sie auf **+**, um einen anderen Wert zuzuordnen.

  4 Klicken Sie abschließend auf **OK**.

- Falls **Benutzerdefinierte Zuordnung** ausgewählt ist, geben Sie den **Wert** ein, der zum Ticket hinzugefügt werden soll.

7 Klicken Sie auf **+**, um ein weiteres Ticket-Feld zuzuordnen.

Zurückverweisen von Tickets auf den Problemstatus

Sie müssen eine Feldzuordnung zwischen Ticket und Problem mit Rückverweis auf das Statusfeld (den Zustand) des Problems konfigurieren, um den Ticket-Server vollständig zu integrieren.



Da dieser Bereich nur den Ticket-Status/-Zustand zuordnet, werden Sie nicht dazu aufgefordert, die ID zum Statusfeld (zum Zustand) des Problems hinzuzufügen. Dieses Feld ist impliziert.



Quellwerte, zugeordnete Werte und Feld-IDs berücksichtigen Groß- und Kleinschreibung.

Vorgehensweise

Definitionen zu Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

1 Wählen Sie unter **Ticket zurück auf das Problemstatusfeld verweisen** einen **Vorgang** aus.

2 Geben Sie unter **Quellfeld** die ID des Ticket-Feldes ein, das den Status/Zustand des Tickets enthält.

3 Falls unter **Vorgang** die Option **Wertebereich** oder **Ersatz** ausgewählt ist, klicken Sie neben **Werte** auf **Bearbeiten**.

- Falls **Wertebereich** ausgewählt ist, geben Sie Ticket-Werte für das Ticket und anschließend die Beschriftung ein, die durch diesen Bereich im Problem ersetzt wird.

- Falls **Ersatz** ausgewählt ist, geben Sie einen **Quellwert** für das Ticket und anschließend unter **Zugeordneter Wert** den zugeordneten Wert ein, der durch diesen Wert im Problem ersetzt wird.

4 Aktivieren Sie das Kontrollkästchen **Problemkommentare mit Ticket-Kommentaren überschreiben**, wenn Problemkommentare Vorrang haben sollen, und geben Sie dann die ID für das **Ticket-Kommentarfeld** ein, das die Daten im Kommentarfeld des Problems überschreibt.

5 Aktivieren Sie **Tickets können erneut geöffnet werden**, wenn Sie diese Option wünschen.

6 Klicken Sie abschließend auf **Testzuordnung**.

Wenn der Test erfolgreich verläuft, wird in einem Dialogfeld eine Ticket-ID angezeigt. Hierbei handelt es sich um die ID für ein Test-Ticket, das im Ticket-Server erstellt wurde.

7 Führen Sie eine der folgenden Aktionen aus:

- Wenn der Test erfolgreich verlaufen ist, suchen Sie das Ticket im Ticket-Server, und überprüfen Sie, ob alle Werte für den einfachen Problemtyp, einschließlich der Testkommentare, richtig zugeordnet wurden. Klicken Sie anschließend auf **OK**.



Mit der Funktion **Testzuordnung** wird die Zuordnung für den einfachen Problemtyp überprüft – unabhängig vom konfigurierten Problemtyp. Daher enthalten die Tickets eventuell unerwartete Ergebnisse, obwohl die Zuordnungstests für Problemtypen aus anderen Produkterweiterungen (erweiterte Problemtypen) jeweils erfolgreich verlaufen sind. Überprüfen Sie für diese Problemtypen, ob Tickets, die nach der vollständigen Integration des Ticket-Servers zu Problemen hinzugefügt wurden, ordnungsgemäß erstellt werden.

- Falls der Text erfolgreich verlaufen ist, überprüfen Sie die Zuordnungen und den Status des Ticket-Servers.

8 Klicken Sie nach Abschluss der Zuordnungstests auf **Speichern**.



Selbst bei einem Fehlschlagen des Zuordnungstests können Sie die Konfiguration speichern und den Server registrieren.

9 Klicken Sie abschließend auf **Speichern**.

Aktualisieren eines registrierten Ticket-Servers

Wenn Sie bei Ihrem Ticket-Server ein Upgrade durchführen, müssen Sie möglicherweise die Integration des vorhandenen Ticket-Servers ändern, damit er weiter funktioniert.



Wird der Server-Task, der mit einem Ticket gekennzeichnete Probleme synchronisiert, nach dem Ändern oder Löschen eines vorhandenen registrierten Ticket-Servers, jedoch vor der Integration des aktualisierten Ticket-Servers ausgeführt, so wird die Ticket/Problem-Zuordnung unterbrochen. Führen Sie in diesem Fall diesen Task aus, und fügen Sie dann manuell Tickets zu allen zuvor mit einem Ticket gekennzeichneten Problemen hinzu. Hierdurch wird die Funktion zum erneuten Öffnen von Tickets ausgeführt. Weitere Informationen finden Sie in diesem Handbuch im Abschnitt zum erneuten Öffnen von Tickets.

Vorgehensweise

1 Führen Sie die folgenden Schritte durch, um den Server-Task zu deaktivieren, der mit einem Ticket gekennzeichnete Probleme synchronisiert.

a Klicken Sie auf **Menü** | **Automatisierung** | **Server-Tasks**, und klicken Sie dann auf den Server-Task "Problemsynchronisierung". Die Seite **Beschreibung** des **Generators für Server-Tasks** wird angezeigt.

b Klicken Sie neben **Planungsstatus** auf **Deaktiviert**.

c Klicken Sie auf **Speichern**.

2 Stellen Sie sicher, dass keine Instanzen des Server-Tasks ausgeführt werden. Falls eine Instanz ausgeführt wird, warten Sie, bis sie beendet wurde, oder brechen Sie sie ab, bevor Sie fortfahren.

3. Führen Sie eine der folgenden Aktionen aus:
   - Bearbeiten Sie den vorhandenen registrierten Ticket-Server basierend auf den Konfigurationsanforderungen für den aktualisierten Ticket-Server.
   - Löschen Sie den vorhandenen registrierten Ticket-Server, und erstellen Sie dann basierend auf den Konfigurationsanforderungen für den aktualisierten Ticket-Server einen neuen Ticket-Server.

   Weitere Informationen finden Sie in diesem Handbuch in den Abschnitten zum Integrieren von Ticket-Servern, zum Installieren von Erweiterungen für Ticket-Server sowie zum Registrieren und Konfigurieren eines Ticket-Servers.
4. Nachdem Sie die Integration in den aktualisierten Ticket-Server konfiguriert haben, aktivieren Sie den Server-Task, der mit einem Ticket gekennzeichnete Probleme synchronisiert.

21 ePolicy Orchestrator-Protokolldateien

Der ePolicy Orchestrator-Server verfügt über Protokolldateien, in denen verschiedene Arten von Ereignissen und Aktionen aufgezeichnet werden, die im System stattfinden.

Inhalt

Das Audit-Protokoll

Mithilfe des Audit-Protokolls können Sie eine Aufzeichnung aller McAfee ePO-Benutzeraktionen aufrufen und verwalten. Die Einträge im Audit-Protokoll werden in einer sortierbaren Tabelle angezeigt. Zwecks größerer Flexibilität können Sie das Protokoll auch so filtern, dass nur fehlgeschlagene Aktionen oder nur Einträge eines bestimmten Alters angezeigt werden.

Das Audit-Protokoll besteht aus sieben Spalten:

- **Aktion** – Der Name der Aktion, die der McAfee ePO-Benutzer auszuführen versuchte.
- **Endzeit** – Der Zeitpunkt, zu dem die Aktion abgeschlossen wurde.
- **Details** – Weitere Informationen zur Aktion.
- **Priorität** – Die Bedeutung der Aktion.
- **Startzeit** – Der Zeitpunkt, zu dem die Aktion gestartet wurde.
- **Erfolgreich** – Gibt an, ob die Aktion erfolgreich abgeschlossen wurde.
- **Benutzername** – Der Benutzername des angemeldeten Benutzerkontos, mit dem die Aktion ausgeführt wurde.

Die Einträge im Audit-Protokoll können abgefragt werden. Sie können mit dem Abfragen-Generator Abfragen für diese Daten erstellen oder die Standardabfragen für diese Daten verwenden. Die Abfrage **Fehlgeschlagene Anmeldeversuche** ruft beispielsweise eine Tabelle aller fehlgeschlagenen Anmeldeversuche ab.

Anzeigen und Bereinigen des Audit-Protokolls

Sie können einen Verlauf von Administratoraktionen anzeigen und bereinigen.

Welche Daten beim Anzeigen des Audit-Protokolls verfügbar sind, hängt davon ab, wie oft und bei welchem Alter das Audit-Protokoll bereinigt wird.



Beim Bereinigen des Audit-Protokolls werden die Datensätze dauerhaft gelöscht.

Vorgehensweise

Definitionen zu Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

1. Klicken Sie auf **Menü** | **Benutzerverwaltung** | **Audit-Protokoll**. Die Audit-Protokolle werden angezeigt.
2. Wählen Sie eine der folgenden Aktionen aus.

Aktion	Vorgehensweise
Anzeigen des Audit-Protokolls	1 Klicken Sie auf einen Spaltentitel, um die Tabelle nach der betreffenden Spalte (alphabetisch) zu sortieren. 2 Wählen Sie in der Dropdown-Liste **Filter** eine Option aus, um die angezeigte Datenmenge einzugrenzen. Sie können alle Aktionen bis auf die fehlgeschlagenen entfernen oder nur die Aktionen anzeigen, die in einem ausgewählten Zeitrahmen erfolgten. 3 Klicken Sie auf einen Eintrag, um dessen Details anzuzeigen.
Bereinigen des Audit-Protokolls	1 Klicken Sie auf **Aktionen** | **Bereinigen**. 2 Geben Sie im Dialogfeld **Bereinigen** neben **Datensätze bereinigen, die älter sind als** eine Zahl ein, und wählen Sie eine Zeiteinheit aus. 3 Klicken Sie auf **OK**. Alle Datensätze im Audit-Protokoll werden dauerhaft gelöscht.

Planmäßiges Bereinigen des Audit-Protokolls

Mit einem geplanten Server-Task können Sie das Audit-Protokoll automatisch bereinigen.

Vorgehensweise

Definitionen zu Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

1. Klicken Sie auf **Menü** | **Automatisierung** | **Server-Tasks**, und klicken Sie dann auf **Aktionen** | **Neuer Task**. Der Assistent **Generator für Server-Tasks** wird mit der Seite **Beschreibung** geöffnet.
2. Geben Sie einen Namen und eine Beschreibung zum Task ein, und klicken Sie neben **Planungsstatus** auf **Aktiviert**.
3. Klicken Sie auf **Weiter**. Die Seite **Aktionen** wird angezeigt.
4. Wählen Sie in der Dropdown-Liste die Option **Audit-Protokoll bereinigen** aus.
5. Geben Sie hinter **Datensätze bereinigen, die älter sind als** eine Zahl ein, und wählen Sie eine Zeiteinheit aus. Sie legen damit fest, welche Audit-Protokolleinträge bereinigt werden sollen.
6. Klicken Sie auf **Weiter**. Die Seite **Plan** wird angezeigt.
7. Planen Sie den Task nach Bedarf, und klicken Sie dann auf **Weiter**. Die Seite **Zusammenfassung** wird angezeigt.
8. Überprüfen Sie die Task-Details, und klicken Sie dann auf **Speichern**.

Das Server-Task-Protokoll

Im Server-Task-Protokoll werden Ereignisse aufgezeichnet, die auf dem ePolicy Orchestrator-Server auftreten.

Im Server-Task-Protokoll können Sie die detaillierten Ergebnisse geplanter Server-Tasks anzeigen, die auf dem Server ausgeführt wurden oder werden.

Einträge in dem Protokoll enthalten Einzelheiten zu den folgenden Punkten:

- Erfolg oder Fehler des Tasks
- Alle Sub-Tasks, die während der Ausführung des geplanten Tasks ausgeführt wurden.

Sie können einen Task, der gerade ausgeführt wird, auch beenden.

Verwalten des Server-Task-Protokolls

Nachdem Sie das Server-Task-Protokoll geöffnet haben, können Sie die Task-Protokolle je nach Bedarf anzeigen, filtern und bereinigen.

Der Status jedes Server-Tasks wird in der Spalte **Status** angezeigt:

- **Wartet** – Der Task wartet darauf, dass ein anderer Task abgeschlossen wird.
- **Wird ausgeführt** – Der Task wurde gestartet, aber noch nicht abgeschlossen.
- **Pausiert** – Der Task wurde durch eine Server-Task-Aktion pausiert.
- **Angehalten** – Der Task wurde durch eine Server-Task-Aktion angehalten.
- **Fehlgeschlagen** – Der Task wurde gestartet, aber nicht erfolgreich abgeschlossen.
- **Abgeschlossen** – Der Task wurde erfolgreich abgeschlossen.
- **Ausstehende Beendigung** – Eine Beendigungsanforderung wurde gesendet.
- **Beendet** – Der Task wurde vor seinem Abschluss manuell beendet.

Vorgehensweise

Definitionen zu Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

1. Klicken Sie auf **Menü** | **Automatisierung** | **Server-Task-Protokoll**. Die Seite **Server-Task-Protokoll** wird angezeigt.
2. Wählen Sie eine der folgenden Aktionen aus.

Aktion	Vorgehensweise
Anzeigen des Server-Task-Protokolls	1 Klicken Sie auf einen Spaltentitel, um die Ereignisse zu sortieren. 2 Wählen Sie eines der Task-Protokolle aus, klicken Sie auf **Aktionen**, und wählen Sie eine der folgenden Optionen zum Ändern des Server-Task-Protokolls aus: • **Spalten auswählen** – Die Seite **Spalten zum Anzeigen auswählen** wird angezeigt. • **Tabelle exportieren** – Die Seite **Exportieren** wird angezeigt. • **Bereinigen** – Das Dialogfeld **Bereinigen** wird angezeigt. Geben Sie mit einer Zahl und einer Zeiteinheit an, welche Task-Protokolleinträge gelöscht werden sollen, und klicken Sie dann auf **OK**. • **Task beenden** – Beendet einen Task, der gerade ausgeführt wird.
Filtern des Server-Task-Protokolls	Wählen Sie in der Dropdown-Liste **Filter** den gewünschten Filter aus.
Bereinigen des Server-Task-Protokolls	1 Klicken Sie auf **Aktionen | Bereinigen**. 2 Geben Sie im Dialogfeld **Bereinigen** eine Anzahl von Tagen, Wochen, Monaten oder Jahren ein. Alle Elemente, die mindestens so alt sind, werden gelöscht. 3 Klicken Sie auf **OK**.

3. Klicken Sie auf einen Spaltentitel, um die Ereignisse zu sortieren.
4. Wählen Sie eines der Task-Protokolle aus, klicken Sie auf **Aktionen**, und wählen Sie eine der folgenden Optionen zum Ändern des Server-Task-Protokolls aus:
   - **Spalten auswählen** – Die Seite **Spalten zum Anzeigen auswählen** wird angezeigt.
   - **Tabelle exportieren** – Die Seite **Exportieren** wird angezeigt.
   - **Bereinigen** – Das Dialogfeld **Bereinigen** wird angezeigt. Geben Sie mit einer Zahl und einer Zeiteinheit an, welche Task-Protokolleinträge gelöscht werden sollen, und klicken Sie dann auf **OK**.
   - **Task beenden** – Beendet einen Task, der gerade ausgeführt wird.

Das Bedrohungsereignisprotokoll

Mithilfe des Bedrohungsereignisprotokolls können Sie Ereignisse in der Datenbank schnell anzeigen und sortieren. Das Protokoll kann nur nach Alter bereinigt werden.

Sie können wählen, welche Spalten in der sortierbaren Tabelle angezeigt werden sollen. Es steht eine Vielzahl von Ereignisdaten als Spalten zur Auswahl.

Je nach den verwalteten Produkten können Sie auch mit bestimmten Aktionen auf die Ereignisse reagieren. Aktionen sind im Menü **Aktionen** unten auf der Seite verfügbar.

Einheitliches Ereignisformat

In den meisten verwalteten Produkten kommt nun ein einheitliches Ereignisformat zum Einsatz. Die Felder dieses Formats können als Spalten im Bedrohungsereignisprotokoll verwendet werden. Dazu gehören:

- **Ausgeführte Aktion** – Die Aktion, die vom Produkt als Reaktion auf die Bedrohung ausgeführt wurde.
- **Agenten-GUID** – Die eindeutige Kennung des Agenten, von dem das Ereignis weitergeleitet wurde.
- **DAT-Version** – Die DAT-Version auf dem System, von dem das Ereignis gesendet wurde.
- **Hostname des entdeckenden Produkts** – Der Name des Systems, auf dem das entdeckende Produkt gehostet ist.
- **ID des entdeckenden Produkts** – Die ID des entdeckenden Produkts.
- **IPv4-Adresse des entdeckenden Produkts** – Die IPv4-Adresse des Systems, auf dem das entdeckende Produkt gehostet ist (sofern zutreffend).
- **IPv6-Adresse des entdeckenden Produkts** – Die IPv6-Adresse des Systems, auf dem das entdeckende Produkt gehostet ist (sofern zutreffend).
- **MAC-Adresse des entdeckenden Produkts** – Die MAC-Adresse des Systems, auf dem das entdeckende Produkt gehostet ist.
- **Name des entdeckenden Produkts** – Der Name des entdeckenden Produkts, das verwaltet wird.
- **Version des entdeckenden Produkts** – Die Versionsnummer des entdeckenden Produkts.
- **Scan-Modul-Version** – Die Versionsnummer des Scan-Moduls des entdeckenden Produkts (sofern zutreffend).
- **Ereigniskategorie** – Die Kategorie des Ereignisses. Die mögliche Kategorien hängen vom Produkt ab.
- **Zeit der Ereignisgenerierung (UTC)** – Der Zeitpunkt, zu dem das Ereignis entdeckt wurde (in koordinierter Weltzeit).
- **Ereignis-ID** – Die eindeutige Kennung des Ereignisses.
- **Zeit des Ereignisempfangs (UTC)** – Der Zeitpunkt, zu dem das Ereignis vom McAfee ePO-Server empfangen wurde (in koordinierter Weltzeit).
- **Dateipfad** – Der Dateipfad des Systems, von dem das Ereignis gesendet wurde.
- **Hostname** – Der Name des Systems, von dem das Ereignis gesendet wurde.
- **IPv4-Adresse** – Die IPv4-Adresse des Systems, von dem das Ereignis gesendet wurde.
- **IPv6-Adresse** – Die IPv6-Adresse des Systems, von dem das Ereignis gesendet wurde.
- **MAC-Adresse** – Die MAC-Adresse des Systems, von dem das Ereignis gesendet wurde.
- **Netzwerkprotokoll** – Das Bedrohungszielprotokoll bei Netzwerk-Bedrohungsklassen.
- **Portnummer** – Der Bedrohungszielport bei Netzwerk-Bedrohungsklassen.
- **Prozessname** – Der Name des Zielprozesses (sofern zutreffend).
- **Server-ID** – Die ID des Servers, von dem das Ereignis gesendet wurde.
- **Name der Bedrohung** – Der Name der Bedrohung.
- **Hostname der Bedrohungsquelle** – Der Name des Systems, von dem die Bedrohung stammt.
- **IPv4-Adresse der Bedrohungsquelle** – Die IPv4-Adresse des Systems, von dem die Bedrohung stammt.

- **IPv6-Adresse der Bedrohungsquelle** – Die IPv6-Adresse des Systems, von dem die Bedrohung stammt.
- **MAC-Adresse der Bedrohungsquelle** – Die MAC-Adresse des Systems, von dem die Bedrohung stammt.
- **URL der Bedrohungsquelle** – Der URL des Systems, von dem die Bedrohung stammt.
- **Benutzername der Bedrohungsquelle** – Der Name des Benutzers, von dem die Bedrohung stammt.
- **Typ der Bedrohung** – Die Klasse der Bedrohung.
- **Benutzername** – Der Benutzername oder die E-Mail-Adresse der Bedrohungsquelle.

Anzeigen und Bereinigen des Bedrohungsereignisprotokolls

Sie sollten Ihre Bedrohungsereignisse in regelmäßigen Abständen anzeigen und bereinigen.

Vorgehensweise

Definitionen zu Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

1 Klicken Sie auf **Menü** | **Berichterstellung** | **Bedrohungsereignisprotokoll**.

2 Wählen Sie eine der folgenden Aktionen aus.

Aktion	Vorgehensweise
Anzeigen des Bedrohungsereignisprotokolls	1 Klicken Sie auf einen Spaltentitel, um die Ereignisse zu sortieren. Sie können auch auf **Aktionen** | **Spalten auswählen** klicken. Daraufhin wird die Seite **Spalten zum Anzeigen auswählen** angezeigt. 2 Wählen Sie in der Liste **Verfügbare Spalten** die Tabellenspalten aus, die Sie benötigen, und klicken Sie dann auf **Speichern**. 3 Wählen Sie Ereignisse in der Tabelle aus, klicken Sie dann auf **Aktionen**, und wählen Sie **Verwandte Systeme anzeigen** aus, um die Details der Systeme anzuzeigen, die die ausgewählten Ereignisse gesendet haben.
Bereinigen von Bedrohungsereignissen	1 Klicken Sie auf **Aktionen** | **Bereinigen**. 2 Geben Sie im Dialogfeld **Bereinigen** neben **Datensätze bereinigen, die älter sind als** eine Zahl ein, und wählen Sie eine Zeiteinheit aus. 3 Klicken Sie auf **OK**. Datensätze, die das angegebene Alter überschritten haben, werden dauerhaft gelöscht.

Planen der Bereinigung des Bedrohungsereignisprotokolls

Sie können einen Server-Task erstellen, mit dem das Bedrohungsereignisprotokoll automatisch bereinigt wird.

Vorgehensweise

Definitionen zu Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

1 Klicken Sie auf **Menü** | **Automatisierung** | **Server-Tasks**, und klicken Sie dann auf **Aktionen** | **Neuer Task**. Der Assistent **Generator für Server-Tasks** wird mit der Seite **Beschreibung** geöffnet.

2 Geben Sie einen Namen und eine Beschreibung zum Task ein, und klicken Sie neben **Planungsstatus** auf **Aktiviert**.

3 Klicken Sie auf **Weiter**. Die Seite **Aktionen** wird angezeigt.

4. Wählen Sie in der Dropdown-Liste die Option **Bedrohungsereignisprotokoll bereinigen** aus.
5. Legen Sie fest, ob nach Alter oder anhand von Abfrageergebnissen bereinigt werden soll. Wenn Sie nach Abfrage bereinigen, müssen Sie eine Abfrage auswählen, deren Ergebnis eine Tabelle mit Ereignissen ist.
6. Klicken Sie auf **Weiter**. Die Seite **Plan** wird angezeigt.
7. Planen Sie den Task nach Bedarf, und klicken Sie dann auf **Weiter**. Die Seite **Zusammenfassung** wird angezeigt.
8. Überprüfen Sie die Task-Details, und klicken Sie dann auf **Speichern**.

22 Wiederherstellung nach Systemausfall

Mit der Funktion "Wiederherstellung nach Systemausfall" können Sie ePolicy Orchestrator schnell wiederherstellen oder erneut installieren. Diese Funktion verwendet Snapshots, um die ePolicy Orchestrator-Konfiguration sowie Erweiterungen, Schlüssel und andere Informationen in regelmäßigen Abständen in Snapshot-Datensätzen in der ePolicy Orchestrator-Datenbank zu speichern.

Inhalt

Was ist eine Wiederherstellung nach einem Systemausfall?

Die ePolicy Orchestrator-Funktion für Wiederherstellungen nach einem Systemausfall speichert bestimmte Datenbankeinträge zum McAfee ePO-Server mithilfe von Snapshots in der Microsoft SQL Server-Datenbank von ePolicy Orchestrator.

Die von den Snapshots gespeicherten Datensätze enthalten die gesamte zum Zeitpunkt der Snapshot-Erstellung vorliegende ePolicy Orchestrator-Konfiguration. Sobald die Snapshot-Datensätze in der Datenbank gespeichert sind, können Sie mithilfe der Microsoft SQL Server-Sicherungsfunktion die gesamte ePolicy Orchestrator-Datenbank speichern und zwecks Wiederherstellung von ePolicy Orchestrator auf einem anderen SQL-Server wiederherstellen.

Beispiele für Verbindungen der SQL-Wiederherstellungs-Datenbank

Mithilfe des wiederhergestellten ePolicy Orchestrator-SQL-Datenbank-Servers, auf dem sich der Snapshot für die Wiederherstellung nach einem Systemausfall befindet, können Sie eine Verbindung zu folgenden Servern herstellen:

- Wiederhergestellte McAfee ePO-Server-Hardware mit dem ursprünglichen Server-Namen und der ursprünglichen IP-Adresse – Dadurch haben Sie zum Beispiel die Möglichkeit, ePolicy Orchestrator nach einem fehlgeschlagenen Upgrade wiederherzustellen.
- Neue McAfee ePO-Server-Hardware mit dem ursprünglichen Server-Namen und der ursprünglichen IP-Adresse – Dadurch können Sie Server-Hardware problemlos aufrüsten oder wiederherstellen, um dann schnell die Verwaltung Ihrer Netzwerksysteme wieder aufzunehmen.

- Neue McAfee ePO-Server-Hardware mit einem neuen Server-Namen und einer neuen IP-Adresse – Auf diese Weise können Sie zum Beispiel Ihren Server aus einer Domäne in eine andere verschieben.



Dieses Beispiel ist auch als vorübergehende Lösung für die Netzwerkverwaltung geeignet, während Sie die McAfee ePO-Server-Hardware und -Software wieder zurück in die ursprüngliche Domäne verschieben und dort installieren.

- Wiederhergestellte oder neue McAfee ePO-Server-Hardware mit mehreren Netzwerkkarten – Dabei müssen Sie darauf achten, dass für die Netzwerkkarte des McAfee ePO-Servers die korrekte IP-Adresse konfiguriert ist.

Der Snapshot-Vorgang ist je nach Version Ihrer SQL-Datenbank so konfiguriert, dass er täglich automatisch ausgeführt wird. Durch Konfiguration eines Skripts, mit dem die SQL-Sicherung automatisch ausgeführt und die SQL-Sicherungsdatei auf den SQL-Datenbank-Wiederherstellungs-Server kopiert wird, können Sie Ihren McAfee ePO-Server noch einfacher wiederherstellen. Darüber hinaus können Sie Snapshots auch manuell erstellen oder Skripte manuell ausführen, um ePolicy Orchestrator nach komplizierten oder wichtigen Änderungen schnell zu sichern.



Mit dem Monitor der Snapshots zur Wiederherstellung nach einem Systemausfall im ePolicy Orchestrator-Dashboard können Sie Ihre Snapshots zentral verwalten und überwachen.

Komponenten für die Wiederherstellung nach einem Systemausfall

Für die Wiederherstellung von ePolicy Orchestrator nach einem Systemausfall sind bestimmte Anforderungen hinsichtlich der Hard- und Software, der Zugriffsberechtigungen sowie der Informationen zu beachten.

Sie benötigen zwei Server-Hardware-Plattformen:

- Ihre vorhandene McAfee ePO-Server-Hardware (nachfolgend als "primärer" McAfee ePO-Server bezeichnet).
- Eine duplizierte SQL-Server-Hardware (nachfolgend als "Wiederherstellungs"-Server bezeichnet, auf dem eine zur primären McAfee ePO-Server-Datenbank passende Version von Microsoft SQL Server ausgeführt wird). Dieser Wiederherstellungs-Server sollte mittels Snapshot- und Microsoft SQL-Sicherungsprozessen immer auf dem aktuellsten Konfigurationsstand des primären McAfee ePO-Servers und der SQL-Datenbank gehalten werden.



Damit es beim Sichern und Wiederherstellen nicht zu Problemen kommt, sollten die Hardware des primären und des Wiederherstellungs-Servers sowie die SQL-Versionen möglichst übereinstimmen.

Snapshot-Monitor im Dashboard

Mithilfe des Monitors **Server-Snapshot** im ePolicy Orchestrator-Dashboard können Sie Ihre Snapshots zentral verwalten und überwachen.



Wenn der Monitor der Snapshots nicht in Ihrem Dashboard angezeigt wird, erfahren Sie unter *Verwalten von Dashboards*, wie Sie ein neues Dashboard erstellen und den Snapshot-Monitor hinzufügen können.

Mithilfe des Monitors **Server-Snapshot** können Sie Folgendes durchführen:

- Klicken Sie auf **Snapshot erstellen**, um ein Snapshot eines McAfee ePO-Servers manuell zu speichern.
- Klicken Sie auf **Siehe Details der letzten Ausführung**, um die Seite **Server-Task-Protokoll: Details** zu öffnen. Auf dieser Seite werden Informationen und Protokolleinträge zu dem letzten gespeicherten Snapshot angezeigt.
- Überprüfen Sie neben **Zeitpunkt der letzten Ausführung** den Zeitpunkt (d. h. Datum und Uhrzeit), zu dem der letzte Snapshot in der SQL-Datenbank gespeichert wurde.
- Klicken Sie auf den Link **Wiederherstellung nach Systemausfall**, um die Hilfeseite mit Informationen zur Wiederherstellung nach einem Systemausfall anzuzeigen.

Die Farbe und der Titel des Snapshot-Monitors geben Aufschluss über den Status Ihres letzten Snapshots. Beispiele:

- **Blau, Snapshot wird in Datenbank gespeichert** – Der Snapshot-Prozess wird gerade durchgeführt.
- **Grün, Snapshot in Datenbank gespeichert** – Der Snapshot-Prozess wurde erfolgreich abgeschlossen, und der Snapshot ist auf dem aktuellen Stand.
- **Rot, Fehler bei Snapshot** – Während des Snapshot-Prozesses ist ein Fehler aufgetreten.
- **Grau, Kein Snapshot verfügbar** – Es wurde kein Snapshot für eine Wiederherstellung nach einem Systemausfall gespeichert.
- **Orange, Snapshot veraltet** – An der Konfiguration wurden Änderungen vorgenommen, und es wurde kein neuer Snapshot gespeichert. Der Status "Snapshot veraltet" wird durch folgende Änderungen verursacht:
  - Eine Erweiterung wurde geändert (z. B. aktualisiert, entfernt, gelöscht, durch eine neuere oder ältere Version ersetzt).
  - Der Ordner "Keystore" wurde geändert.
  - Der Ordner "conf" wurde geändert.
  - Die Passphrase für die Wiederherstellung nach einem Systemausfall wurde in den Server-Einstellungen geändert.

Task "Server-Snapshot für Wiederherstellung nach Systemausfall"

Mit dem Task "Server-Snapshot für Wiederherstellung nach Systemausfall" können Sie den Plan für den Task zum Erstellen eines Server-Snapshots aktivieren oder deaktivieren.



Der Plan für den Task zum Erstellen eines Server-Snapshots ist bei der Microsoft SQL Server-Datenbank standardmäßig aktiviert, bei der Datenbank von Microsoft SQL Server Express Edition hingegen standardmäßig deaktiviert.

Anforderungen für eine Wiederherstellung nach einem Systemausfall

Für eine Wiederherstellung nach einem Systemausfall müssen die in der folgenden Tabelle aufgeführten Anforderungen hinsichtlich Hard- und Software sowie der Informationen erfüllt sein.

Anforderung	Beschreibung
Hardware-Anforderungen	
Hardware des primären McAfee ePO-Servers	Die Anforderungen an die Server-Hardware hängen von der Anzahl der verwalteten Systeme ab. So können der McAfee ePO-Server und die SQL Server-Datenbank auf der gleichen oder auf unterschiedlicher Hardware installiert sein. Ausführliche Informationen zu den Hardware-Anforderungen finden Sie im *Installationshandbuch von ePolicy Orchestrator 5.0.0*.
Hardware des McAfee ePO-Wiederherstellungs-Servers	Diese Server-Hardware sollte möglichst identisch mit der Hardware des primären McAfee ePO-Servers sein.
Primärer McAfee ePO-Server	Der primäre Server sollte mit einem kürzlich in der SQL-Datenbank gespeicherten Snapshot ordnungsgemäß laufen.
Primäre SQL-Datenbank	In der primären SQL-Datenbank werden die McAfee ePO-Server-Konfiguration, die Client-Informationen sowie die Datensätze aus dem Snapshot für die Wiederherstellung nach einem Systemausfall gespeichert.
Software-Anforderungen	
Sicherungsdatei der primären SQL-Datenbank	Eine Sicherungsdatei der primären Datenbank, die auch die Snapshot-Datensätze umfasst, können Sie entweder mithilfe von Microsoft SQL Server Management Studio oder der BACKUP-Befehlszeile (Transact-SQL) erstellen.
Software der SQL-Wiederherstellungs-Datenbank	Die primäre Datenbank mit den Snapshot-Datensätzen können Sie entweder mithilfe von Microsoft SQL Server Management Studio oder der RESTORE-Befehlszeile (Transact-SQL) auf dem SQL-Datenbank-Wiederherstellungs-Server wiederherstellen, um die Konfiguration der primären SQL-Datenbank zu duplizieren.
ePolicy Orchestrator	Mit dieser von der McAfee-Website heruntergeladenen Software wird der McAfee ePO-Wiederherstellungs-Server installiert und konfiguriert.
Erforderliche Informationen	
Passphrase für die Schlüsselspeicherverschlüsselung zur Wiederherstellung nach einem Systemausfall	Diese Passphrase wurde während der Erstinstallation von ePolicy Orchestrator hinzugefügt und entschlüsselt die vertraulichen Informationen, die im Snapshot für die Wiederherstellung nach einem Systemausfall gespeichert sind. Die Vorgehensweise zum Festlegen der Passphrase für die Schlüsselspeicherverschlüsselung wird unter *Konfigurieren von Server-Einstellungen zur Wiederherstellung nach einem Systemausfall* beschrieben.
Administratorrechte	Sie müssen Zugriff auf den primären und den Wiederherstellungs-Server sowie auf die SQL-Datenbank (z. B. als "DBOwner" und "DBCreator") haben.

Anforderung	Beschreibung
Die letzte bekannte Netzwerkadresse (IP-Adresse, DNS-Name oder NetBIOS-Name) des primären McAfee ePO-Servers	Wenn Sie während der Wiederherstellung des McAfee ePO-Servers eine dieser Einstellungen ändern, müssen Sie sicherstellen, dass McAfee Agent eine Möglichkeit hat, den Server zu finden. Am einfachsten erstellen Sie dazu einen CNAME-Eintrag im DNS, der Anfragen, die an die alte Adresse (IP-Adresse, DNS-Name oder NetBIOS-Name) des primären McAfee ePO-Servers gerichtet sind, auf die neuen Informationen des McAfee ePO-Wiederherstellungs-Server verweist. Informationen dazu finden Sie unter *Ermitteln der vorhandenen IP-Adresse sowie des vorhandenen DNS- und Datenbanknamens*.
Informationen zur Cluster-Umgebung	(Wird noch geschrieben)

Ermitteln der vorhandenen IP-Adresse sowie des vorhandenen DNS- und Datenbanknamens

Die IP-Adresse, den DNS-Namen und den Namen der Datenbank Ihres McAfee ePO-Servers sollten Sie sich am besten notieren, bevor es zu einem Systemausfall kommt, da Sie diese Informationen eventuell während der Wiederherstellung nach einem Systemausfall benötigen.

Ermitteln des Servers und des Namens der Microsoft SQL-Datenbank mithilfe eines Remote-Befehls

Mit dem folgenden Remote-Befehl von ePolicy Orchestrator können Sie den Server und den Namen der Microsoft SQL-Datenbank ermitteln.

1. Geben Sie den folgenden Remote-Befehl in die Adresszeile eines Web-Browsers ein:

   `https://localhost:8443/core/config`

   Dabei ist:

   - `localhost` – Der Name Ihres McAfee ePO-Servers.
   - `:8443` – Der Standardport des McAfee ePO-Servers. Ihr Server kann auch für die Verwendung einer anderen Portnummer konfiguriert sein.

2. Speichern Sie die folgenden Informationen, die auf der Seite **Datenbankeinstellungen konfigurieren** angezeigt werden:

   - **Hostname oder IP-Adresse**
   - **Datenbankname**

Diese Informationen werden im nächsten Abschnitt benötigt.

Ermitteln von Informationen über den McAfee ePO-Server mithilfe von Microsoft SQL Server Management Studio

Gehen Sie in Microsoft SQL Server Management Studio wie folgt vor, um Informationen zu Ihrem vorhandenen McAfee ePO-Server zu ermitteln:

1. Melden Sie sich auf eine beliebige Weise (z. B. mittels Remote-Desktopverbindung) bei dem Hostnamen oder der IP-Adresse des Microsoft SQL-Datenbank-Servers an, die Sie oben in Schritt 2 ermittelt haben.
2. Öffnen Sie Microsoft SQL Server Management Studio, und stellen Sie eine Verbindung zum SQL-Server her.

3 Klicken Sie in der Liste **Objekt-Explorer** auf ***Name des Datenbank-Servers* | Datenbanken | *Datenbankname* | Tabellen**. Die Liste der Tabellen wird in der Liste **Details zum Objekt-Explorer** angezeigt.



Die Werte für ***Name des Datenbank-Servers*** und ***Datenbankname*** haben Sie im vorherigen Abschnitt in Schritt 2 ermittelt.

4 Führen Sie einen Bildlauf durch, bis Sie die Tabelle **EPOServerInfo** finden. Klicken Sie dann mit der rechten Maustaste auf den Tabellennamen, und wählen Sie in der Liste den Eintrag **Oberste 200 Zeilen bearbeiten** aus.

5 Suchen Sie die Informationen, die in der Datenbank in den folgenden Datensätzen stehen, und speichern Sie sie:

- **ePOVersion** – Zum Beispiel 5.0.0
- **DNSName** – Zum Beispiel epo-2k8-epo50.server.com
- **ComputerName** – Zum Beispiel EPO-2K8-EPO50
- **LastKnownTCPIP** – Zum Beispiel 172.10.10.10
- **RmdSecureHttpPort** – Zum Beispiel 8443

Diese Informationen benötigen Sie, wenn Sie ePolicy Orchestrator wiederherstellen müssen.

Funktionsweise der Wiederherstellung nach einem Systemausfall

Für eine schnelle Neuinstallation von ePolicy Orchestrator müssen in regelmäßigen Abständen Snapshots der ePolicy Orchestrator-Konfiguration erstellt werden. Anschließend muss die Datenbank gesichert und auf einem Wiederherstellungs-Server wiederhergestellt sowie ePolicy Orchestrator mit der Option **Wiederherstellen** neu installiert werden.

Überblick über Snapshots zur Wiederherstellung nach einem Systemausfall und Sicherungen

Mithilfe von Snapshots zur Wiederherstellung nach einem Systemausfall, Sicherungen der SQL-Datenbank und Kopiervorgängen wird ein Duplikat der ePolicy Orchestrator-Datenbank auf einem SQL-Datenbank-Wiederherstellungs-Server erstellt.

In diesem Kapitel erhalten Sie einen Überblick über Snapshots zur Wiederherstellung nach einem Systemausfall, Sicherungen der SQL-Datenbank und Kopiervorgänge. Ausführliche Informationen dazu finden Sie unter:

- *Erstellen eines Snapshots*
- *Sichern und Wiederherstellen von Datenbanken mithilfe von Microsoft SQL Server*

Die folgende Abbildung gibt Ihnen einen Überblick darüber, wie die Wiederherstellung von ePolicy Orchestrator nach einem Systemausfall abläuft und welche Hardware erforderlich ist.



In dieser Abbildung ist die SQL-Datenbank auf dem gleichen Computer wie der McAfee ePO-Server installiert. Der McAfee ePO-Server und die SQL-Datenbank können aber auch auf unterschiedlichen Computern installiert sein.

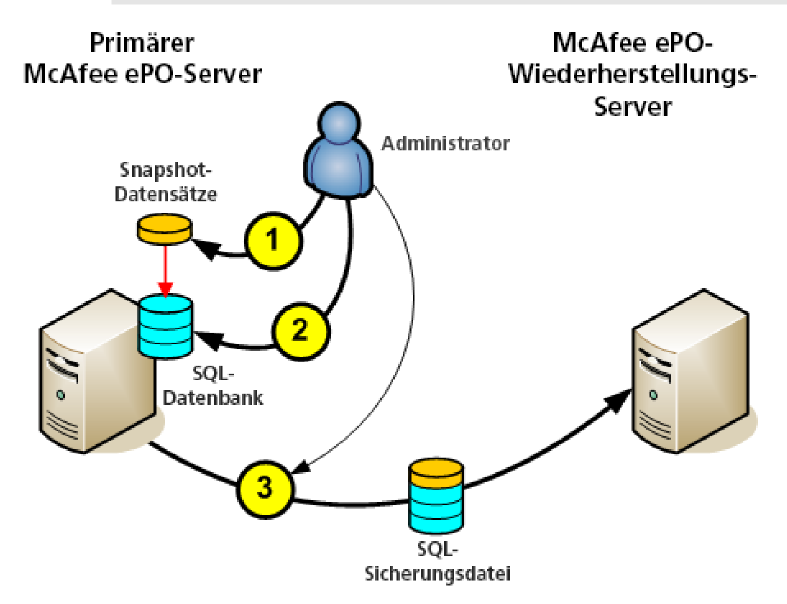


Abbildung 22-1 Snapshot zur Wiederherstellung des McAfee ePO-Servers nach einem Systemausfall und Sicherung

Die Konfiguration der Wiederherstellung von ePolicy Orchestrator nach einem Systemausfall umfasst folgende allgemeine Schritte, die auf dem primären McAfee ePO-Server durchgeführt werden:

1 Erstellen Sie einen Snapshot der McAfee ePO-Server-Konfiguration, und speichern Sie ihn in der primären SQL-Datenbank. Dies kann manuell oder mithilfe eines für diesen Zweck erstellten standardmäßigen Server-Tasks erfolgen.

   In dem erstellten Snapshot werden die folgenden Datenbankdateien gespeichert:

   - C:\Programme\McAfee\ePolicy Orchestrator\Server\extensions – Der Standardpfad zu Informationen über ePolicy Orchestrator-Erweiterungen.
   - C:\Programme\McAfee\ePolicy Orchestrator\Server\conf – Der Standardpfad zu Dateien, die von den ePolicy Orchestrator-Erweiterungen benötigt werden.
   - C:\Programme\McAfee\ePolicy Orchestrator\Server\keystore – Diese Schlüssel sind speziell für die Agent-zu-Server-Kommunikation von ePolicy Orchestrator und die Repositories vorgesehen.

- C:\Programme\McAfee\ePolicy Orchestrator\Server\DB\Keystore – Der Standardpfad zu den Server-Zertifikaten von McAfee-Produktinstallationen.
- C:\Programme\McAfee\ePolicy Orchestrator\Server\DB\Software – Der Standardpfad zu den Installationsdateien von McAfee-Produkten.

  Die gespeicherten Datensätze aus dem Snapshot für die Wiederherstellung nach einem Systemausfall enthalten die Pfade, die Sie für Ihre registrierten ausführbaren Dateien konfiguriert haben. Die registrierten ausführbaren Dateien werden nicht gesichert und müssen von Ihnen beim Wiederherstellen des McAfee ePO-Servers ersetzt werden. Registrierte ausführbare Dateien, deren Pfade nach der Wiederherstellung des McAfee ePO-Servers nicht mehr korrekt sind, werden auf der Seite **Registrierte ausführbare Dateien** rot markiert angezeigt.



Sie sollten die Pfade der registrierten ausführbaren Dateien nach einer Wiederherstellung des McAfee ePO-Servers überprüfen. Auch registrierte ausführbare Dateien, die nicht rot markiert sind, können aufgrund von Abhängigkeitenproblemen Fehler verursachen.

2. Sichern Sie die SQL-Datenbank entweder mithilfe von Microsoft SQL Server Management Studio oder der BACKUP-Befehlszeile (Transact-SQL).
3. Kopieren Sie die in Schritt 2 erstellte Sicherungsdatei für die SQL-Datenbank auf den duplizierten SQL-Wiederherstellungs-Server.



Es ist wichtig, dass Sie die Schritte 2 und 3 abschließen, um die Snapshots vom primären SQL-Server auf den SQL-Wiederherstellungs-Server kopieren und damit die Funktion zur Wiederherstellung nach einem Systemausfall nutzen zu können.

Damit ist die Erstellung und Sicherung des McAfee ePO-Server-Snapshots für Wiederherstellungszwecke nach einem Systemausfall abgeschlossen. Die folgende Wiederherstellungsinstallation des McAfee ePO-Servers müssen Sie nur durchführen, wenn Sie ePolicy Orchestrator neu installieren.

Überblick über eine Wiederherstellungsinstallation des McAfee ePO-Servers

Die Neuinstallation der Software ePolicy Orchestrator ist der letzte Schritt bei einer schnellen Wiederherstellung des McAfee ePO-Servers.

In diesem Abschnitt erhalten Sie einen Überblick über die Neuinstallation von ePolicy Orchestrator auf dem McAfee ePO-Wiederherstellungs-Server. Ausführliche Informationen dazu finden Sie im *Installationshandbuch von ePolicy Orchestrator 5.0.0*.

Die folgende Abbildung zeigt einen Überblick über die Neuinstallation eines McAfee ePO-Servers.



In dieser Abbildung ist die SQL-Datenbank auf dem gleichen Computer wie der McAfee ePO-Server installiert. Der McAfee ePO-Server und die SQL-Datenbank können aber auch auf unterschiedlichen Computern installiert sein.

Primärer McAfee ePO-Server

McAfee ePO-Wiederherstellungs-Server



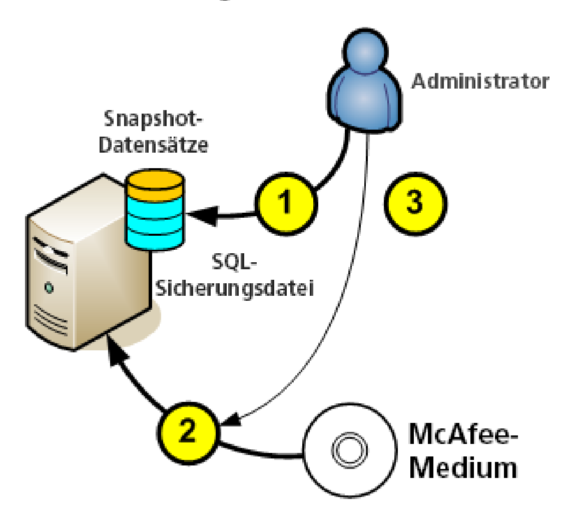


Abbildung 22-2 Wiederherstellungsinstallation eines McAfee ePO-Servers

Bei einer erneuten Installation von ePolicy Orchestrator mithilfe der Snapshot-Datei zur Wiederherstellung nach einem Systemausfall müssen auf dem McAfee ePO-Wiederherstellungs-Server die folgenden allgemeinen Schritte durchgeführt werden:

1. Suchen Sie die Sicherungsdatei der SQL-Datenbank, die Sie im vorherigen Abschnitt in Schritt 3 erstellt haben, und stellen Sie damit die Konfiguration des primären SQL-Servers auf dem SQL-Wiederherstellungs-Server wieder her. Verwenden Sie dabei entweder Microsoft SQL Server Management Studio oder die Methode mit der RESTORE-Befehlszeile (Transact-SQL).

2. Während der Installation der ePolicy Orchestrator-Datenbank-Software:

   a. Klicken Sie im Dialogfeld **Willkommen** auf **ePO aus einem vorhandenen Datenbank-Snapshot wiederherstellen**.

   b. Wählen Sie **Microsoft SQL Server** aus, um ePolicy Orchestrator mit der SQL-Wiederherstellungs-Datenbank zu verknüpfen, die die in Schritt 1 wiederhergestellte Konfiguration des primären McAfee ePO-Servers enthält.

   Nachdem die Installation von ePolicy Orchestrator gestartet wurde, werden keine neuen Einträge in der Datenbank erstellt, sondern die Software wird mithilfe der Einträge konfiguriert, die während der Snapshot-Erstellung in der Datenbank gespeichert wurden.

3. Wenn Sie beim Erstellen des McAfee ePO-Wiederherstellungs-Servers die letzten bekannten Informationen (IP-Adresse, DNS-Name oder NetBIOS-Name) des primären McAfee ePO-Servers geändert haben, kann McAfee Agent keine Verbindung zum wiederhergestellten McAfee ePO-Server aufbauen. Am besten erstellen Sie dann einen CNAME-Eintrag im DNS, der Anfragen, die an die Adresse (IP-Adresse, DNS-Name oder NetBIOS-Name) des primären McAfee ePO-Servers gerichtet sind, auf die neuen Informationen des McAfee ePO-Wiederherstellungs-Servers verweist.

   Unter *Was ist eine Wiederherstellung nach einem Systemausfall?* finden Sie verschiedene Beispiele für das Wiederherstellen der SQL-Datenbankverbindung zum McAfee ePO-Server.

Nun wird der McAfee ePO-Wiederherstellungs-Server mit exakt der gleichen Konfiguration wie der primäre Server ausgeführt. Die Clients können Verbindungen zum Wiederherstellungs-Server aufbauen, und Sie können diese Clients genau wie vor dem Entfernen des primären McAfee ePO-Servers verwalten.

Failback auf die ursprüngliche Server-Site

Nachdem Sie ePolicy Orchestrator und die SQL-Server-Datenbank auf einer neuen Server-Hardware wiederhergestellt haben, möchten Sie möglicherweise ein Failback auf den ursprünglichen primären McAfee ePO-Server durchführen. Wenn sich die Hardware mit dem neuen, wiederhergestellten Server an einem remoten Wiederherstellungsstandort befindet (z. B. in Berlin), möchten Sie diesen Server eventuell nur so lange einsetzen, bis die neue Server-Hardware am alten Standort (z. B. in München) beispielsweise neu installiert oder aufgerüstet wurde.

Zum Durchführen eines Failbacks auf den ursprünglichen primären Server müssen Sie einfach nur die folgenden allgemeinen Schritte durchführen, um von dem McAfee ePO-Server am Remote-Standort (Berlin) wieder zurück zum primären Server (München) zu wechseln:

1. Erstellen Sie einen Snapshot des remoten McAfee ePO-Servers zur Wiederherstellung nach einem Systemausfall, und sichern Sie die SQL-Datenbank.
2. Kopieren Sie die SQL-Datei `ePO_<Server-Name>.bak` vom Remote-Server (in Berlin) zurück auf den primären Server (in München).
3. Installieren Sie ePolicy Orchestrator wieder auf dem primären McAfee ePO-Server (in München).

Nach Abschluss des Failbacks ist der ursprüngliche primäre Server (in München) wieder online, und Sie können den Server am Remote-Standort (in Berlin) weiter als Wiederherstellungs-Server verwenden.

Konfigurieren eines Snapshots und Wiederherstellen der SQL-Datenbank

Für eine schnelle Neuinstallation eines McAfee ePO-Servers müssen Sie einen Snapshot für die Wiederherstellung nach einem Systemausfall konfigurieren und speichern, oder sicherstellen, dass ein Snapshot in der SQL-Datenbank gespeichert wird. Anschließend erstellen Sie eine Sicherung der SQL-Datenbank, in der sich der Snapshot befindet, und kopieren die Datenbank-Sicherungsdatei auf einen SQL-Wiederherstellungs-Server.

Für eine schnelle Neuinstallation eines McAfee ePO-Servers müssen Sie folgende Aufgaben ausführen.

Aufgaben

- *Konfigurieren eines Tasks zur Erstellung eines Server-Snapshots für die Wiederherstellung nach einem Systemausfall* auf Seite 329
  Mithilfe des Tasks "Server-Snapshot für Wiederherstellung nach Systemausfall" können Sie die geplanten automatischen Snapshots einer McAfee ePO-Server-Konfiguration ändern, die in der SQL-Datenbank gespeichert sind.
- *Erstellen eines Snapshots* auf Seite 330
  Regelmäßige Snapshots Ihres primären McAfee ePO-Servers zur Wiederherstellung nach einem Systemausfall sind der erste Schritt, um einen McAfee ePO-Server schnell wiederherstellen zu können.
- *Sichern und Wiederherstellen von Datenbanken mithilfe von Microsoft SQL Server* auf Seite 333
  Zum Speichern des Snapshots für die Wiederherstellung nach einem Systemausfall, in dem sich die Konfigurationsinformationen des McAfee ePO-Servers befinden, werden die Prozeduren von Microsoft SQL Server verwendet.

Konfigurieren eines Tasks zur Erstellung eines Server-Snapshots für die Wiederherstellung nach einem Systemausfall

Mithilfe des Tasks "Server-Snapshot für Wiederherstellung nach Systemausfall" können Sie die geplanten automatischen Snapshots einer McAfee ePO-Server-Konfiguration ändern, die in der SQL-Datenbank gespeichert sind.

Der vorkonfigurierte Status eines Tasks "Server-Snapshot für Wiederherstellung nach Systemausfall" hängt von der SQL-Datenbank ab, die der McAfee ePO-Server verwendet. Bei allen Editionen von Microsoft SQL Server (außer der Express Edition) ist die Snapshot-Funktion für die Wiederherstellung nach einem Systemausfall standardmäßig aktiviert.



Aufgrund der Größenbeschränkungen bei Datendateien in Microsoft SQL Server Express Edition rät McAfee davon ab, die Planung von Snapshots für die Wiederherstellung nach einem Systemausfall zu aktivieren. Bei Microsoft SQL Server 2005 Express Edition beträgt die maximale Dateigröße nur 4 GB und bei Microsoft SQL Server 2008 Express Edition sowie Microsoft SQL Server 2012 Express Edition nur 10 GB.

Es kann immer nur ein Snapshot für die Wiederherstellung nach einem Systemausfall ausgeführt werden. Wenn Sie mehrere Snapshots ausführen, erstellt nur der letzte Snapshot eine Ausgabe, wobei die vorherigen Snapshots überschrieben werden.

Je nach Bedarf können Sie den standardmäßigen Task zur Erstellung eines Server-Snapshots für die Wiederherstellung nach einem Systemausfall ändern.

Vorgehensweise

Definitionen zu Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

1. Klicken Sie auf **Menü | Server-Tasks**, wählen Sie in der Liste **Server-Tasks** den Eintrag **Server-Snapshot für Wiederherstellung nach Systemausfall** aus, und klicken Sie auf **Bearbeiten**.

   Der Assistent für Tasks zur Erstellung eines Server-Snapshots für die Wiederherstellung nach einem Systemausfall wird angezeigt.

2. Klicken Sie auf der Registerkarte **Beschreibungen** unter **Planungsstatus** je nach Bedarf auf **Aktiviert** oder **Deaktiviert**.

3. Ändern Sie auf der Registerkarte **Plan** je nach Bedarf die folgenden Einstellungen:
   - **Planungstyp** – Legt fest, wie häufig der Snapshot gespeichert wird.
   - **Startdatum** und **Enddatum** – Legen Sie das Start- und Enddatum zum Speichern der Snapshots fest, oder klicken Sie auf **Kein Enddatum**, wenn der Task dauerhaft ausgeführt werden soll.
   - **Plan** – Hiermit legen Sie die Uhrzeit fest, zu der der Snapshot gespeichert werden soll. In der Standardeinstellung wird der Snapshot-Task jeden Tag um 01:59 Uhr ausgeführt.

   McAfee empfiehlt, den Task zur Erstellung eines Server-Snapshots für die Wiederherstellung nach einem Systemausfall außerhalb der Spitzenzeiten auszuführen, damit während der Erstellung des Snapshots möglichst wenige Änderungen an der Datenbank vorgenommen werden.

4. Überprüfen Sie auf der Registerkarte **Zusammenfassung**, dass der Server-Task ordnungsgemäß konfiguriert ist, und klicken Sie dann auf **Speichern**.

Erstellen eines Snapshots

Regelmäßige Snapshots Ihres primären McAfee ePO-Servers zur Wiederherstellung nach einem Systemausfall sind der erste Schritt, um einen McAfee ePO-Server schnell wiederherstellen zu können.

Wenn Sie größere Änderungen an der Konfiguration der McAfee-Software vorgenommen haben, sollten Sie mithilfe einer der folgenden Methoden manuell einen Snapshot für die Wiederherstellung nach einem Systemausfall erstellen.



Erstellen Sie zur Automatisierung von Server-Snapshots einen Task "Server-Snapshot für Wiederherstellung nach Systemausfall".

Aufgaben

- *Erstellen von Snapshots im Dashboard* auf Seite 330
  Im ePolicy Orchestrator-Dashboard können Sie für eine eventuelle Wiederherstellung nach einem Systemausfall Snapshots Ihres primären McAfee ePO-Servers erstellen und den Snapshot-Prozess anhand der Statusänderungen im Dashboard überwachen.
- *Erstellen von Snapshots per Web-API* auf Seite 331
  Über die Web-API von ePolicy Orchestrator können Sie für eine eventuelle Wiederherstellung nach einem Systemausfall Snapshots Ihres primären McAfee ePO-Servers erstellen. Bei dieser Methode können Sie den gesamten Vorgang mit einer einzigen Befehlszeile durchführen.

Erstellen von Snapshots im Dashboard

Im ePolicy Orchestrator-Dashboard können Sie für eine eventuelle Wiederherstellung nach einem Systemausfall Snapshots Ihres primären McAfee ePO-Servers erstellen und den Snapshot-Prozess anhand der Statusänderungen im Dashboard überwachen.

Vorgehensweise

Definitionen zu Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

1. Klicken Sie auf **Menü** | **Berichterstellung** | **Dashboards**, um den Monitor **ePO-Server-Snapshot** anzuzeigen.

   Falls erforderlich, klicken Sie auf **Monitor hinzufügen**, wählen in der Liste den Monitor **ePO-Server-Snapshot** aus und ziehen ihn in das Dashboard.

2. Klicken Sie auf **Snapshot erstellen**, um mit dem Speichern der McAfee ePO-Server-Konfiguration zu beginnen.

   Während der Snapshot-Erstellung wird der Status des Vorgangs in der Titelleiste des Snapshot-Monitors angezeigt. Informationen zu den Statusangaben im Snapshot-Monitor finden Sie unter *Snapshot-Monitor im Dashboard*.

   Je nach der Komplexität und Größe des von ePolicy Orchestrator verwalteten Netzwerks kann die Snapshot-Erstellung zwischen 10 Minuten und bis zu mehr als einer Stunde in Anspruch nehmen. Die Leistung des McAfee ePO-Servers sollte dabei nicht beeinträchtigt werden.

3. Wenn gewünscht, klicken Sie auf **Siehe Details der aktuellen Ausführung**, um im Server-Task-Protokoll die Details zum letzten gespeicherten Snapshot anzuzeigen.

   Nach Abschluss des Snapshot-Erstellung klicken Sie auf **Siehe Details der aktuellen Ausführung**, um im Server-Task-Protokoll die Details zum letzten gespeicherten Snapshot anzuzeigen.

Der aktuelle Snapshot für die Wiederherstellung nach einem Systemausfall wird in der primären SQL-Datenbank des McAfee ePO-Servers gespeichert. Nun kann die Datenbank gesichert und auf den SQL-Datenbank-Wiederherstellungs-Server kopiert werden.

Erstellen von Snapshots per Web-API

Über die Web-API von ePolicy Orchestrator können Sie für eine eventuelle Wiederherstellung nach einem Systemausfall Snapshots Ihres primären McAfee ePO-Servers erstellen. Bei dieser Methode können Sie den gesamten Vorgang mit einer einzigen Befehlszeile durchführen.

Alle in diesem Schritt beschriebenen Befehle werden in die Adresszeile Ihres Web-Browsers eingegeben, um remote auf den McAfee ePO-Server zuzugreifen.



Bevor das Ergebnis angezeigt wird, werden Sie zur Eingabe des Adminstratorbenutzernamens und -kennworts aufgefordert.

Ausführliche Informationen über die Nutzung der Web-API und entsprechende Beispiele finden Sie im *Skripthandbuch zu McAfee ePolicy Orchestrator 5.0.0*.

Vorgehensweise

Definitionen zu Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

1 Mit dem folgenden Hilfebefehl der ePolicy Orchestrator-Web-API können Sie die Parameter ermitteln, die zum Ausführen des Snapshots erforderlich sind:

   `https://localhost:8443/remote/core.help?command=scheduler.runServerTask`

   Dabei ist:

   - `localhost` – Der Name Ihres ePolicy Orchestrator-Servers.
   - `8443` – Der Zielport, hier als "8443" (Standardwert) angegeben.
   - `/remote/core.help?command=` – Ruft die Web-API-Hilfe auf.
   - `scheduler.runServerTask` – Ruft die spezielle Server-Task-Hilfe auf.

   Beim Befehl `runServerTask` muss die Groß- und Kleinschreibung berücksichtigt werden.

   Der oben aufgeführte Befehl gibt den folgenden Hilfetext zurück.

```
OK:
scheduler.runServerTask taskName
Führt einen Server-Task aus und gibt anschließend die Task-Protokoll-ID zurück. Mithilfe
der Task-Protokoll-ID können Sie mit dem Befehl 'tasklog.listTaskHistory' den Status des
ausgeführten Tasks anzeigen. Gibt die Liste der Task-Protokoll-ID zurück oder meldet einen
Fehler.
Berechtigung zum Ausführen von Server-Tasks erforderlich.
Parameter:
 [taskName (param 1) | taskId] - Eindeutige Task-ID oder eindeutiger Task-Name
```

2 Mit dem folgenden Befehl können Sie alle Server-Tasks auflisten und den taskName-Parameter ermitteln, der zum Ausführen des Tasks zum Erstellen eines Server-Snapshots erforderlich ist:

```
https://localhost:8443/remote/scheduler.listAllServerTasks?:output=terse
```

Der oben aufgeführte Befehl gibt eine Liste zurück, die in etwa wie folgt aussieht. Wie die Liste im Einzelnen aussieht, hängt von Ihren Berechtigungen und den installierten Erweiterungen ab.

```
OK:
ID Name                                                                  Next Run
-- --------------------------------------------------------------------- -----------------
14 Update Master Repository                                              8/1/12 at 2:17 AM
7  Synchronize Shared Tasks                                              None
6  Synchronize Shared Policies                                           None
11 RSD: Update Sensor Deployment Client Tasks                            None
10 RSD: Default Delete Detected Systems Task                             None
12 Roll Up Data (Local ePO Server)                                       None
8  Purge Threat and Client Events Older than 90 Days                     None
3  Issue synchronization                                                 None
15 Inactive Agent Cleanup Task                                           None
13 Generate Records for McAfee Agent Compliance History Reporting        None
4  Duplicate Agent GUID - remove systems with potentially duplicated GUIDs None
5  Duplicate Agent GUID - clear error count                              None
9  Download Software Product List                                        8/1/12 at 2:09 AM
2  Disaster Recovery Snapshot Server                                     8/1/12 at 1:59 AM
```

3 Führen Sie mit dem folgenden Befehl den Task zum Erstellen eines Server-Snapshots aus. Verwenden Sie dabei den im vorherigen Schritt ermittelten Task-Namen (`Disaster Recovery Snapshot Server`).

```
https://localhost:8443/remote/scheduler.runServerTask?taskName=Disaster%20Recovery
%20Snapshot%20Server
```

Wenn der Task erfolgreich abgeschlossen wird, sieht die Ausgabe wie folgt aus:

```
OK: 102
```



Je nach der Komplexität und Größe des von ePolicy Orchestrator verwalteten Netzwerks kann die Snapshot-Erstellung zwischen 10 Minuten und bis zu mehr als einer Stunde in Anspruch nehmen. Die Leistung des McAfee ePO-Servers sollte dabei nicht beeinträchtigt werden.

4 Überzeugen Sie sich, dass der Web-API-Server-Task zum Erstellen des Snapshots erfolgreich ausgeführt wurde.

a Mit dem folgenden Befehl können Sie die ID des Tasks "Server-Snapshot für Wiederherstellung nach Systemausfall" aus dem Protokoll ermitteln:

```
https://localhost:8443/remote/tasklog.listTaskHistory?taskName=Disaster
%20Recovery%20Snapshot%20Server
```

Dieser Befehl zeigt alle Tasks vom Typ "Server-Snapshot für Wiederherstellung nach Systemausfall" an. Suchen Sie den aktuellsten Task, und notieren Sie sich dessen ID-Nummer. Im Beispiel unten ist das "ID: 102".

```
ID: 102
Name: Server-Snapshot für Wiederherstellung nach Systemausfall
Startdatum: 8/7/12 11:00:34 AM
Enddatum: 8/7/12 11:01:18 AM
Benutzername: admin
Status: Abgeschlossen
Quelle: Planer
Dauer: Weniger als eine Minute
```

b Verwenden Sie den folgenden Befehl mit dieser Task-ID-Nummer 102, um alle zugehörigen Meldungen aus dem Task-Protokoll anzuzeigen.

`https://localhost:8443/remote/tasklog.listMessages?taskLogId=102`

Gehen Sie die Meldungen bis zum Ende durch, und suchen Sie nach dem folgenden Eintrag:

```
OK:
Datum: 8/7/12 11:00:34 AM
Meldung: Server-Snapshot erstellen und in Datenbank speichern

Datum: 8/7/12 11:00:34 AM
Meldung: Speicherung des Server-Snapshots in der Datenbank wird gestartet...

. . .

Datum: 8/7/12 11:01:18 AM
Meldung: Server-Snapshot wurde erfolgreich in der Datenbank gespeichert

Datum: 8/7/12 11:01:18 AM
Meldung: Server-Snapshot erstellen und in Datenbank speichern
```

Sichern und Wiederherstellen von Datenbanken mithilfe von Microsoft SQL Server

Zum Speichern des Snapshots für die Wiederherstellung nach einem Systemausfall, in dem sich die Konfigurationsinformationen des McAfee ePO-Servers befinden, werden die Prozeduren von Microsoft SQL Server verwendet.

Bevor Sie beginnen

Hierfür müssen Sie über Konnektivität sowie über eine Autorisierung verfügen, um Dateien vom primären auf den McAfee ePO-SQL-Wiederherstellungs-Server kopieren zu können. Ausführliche Informationen dazu finden Sie in *Anhang A: Verwalten von ePolicy Orchestrator-Datenbanken*.

Nachdem Sie einen Snapshot der Konfiguration des McAfee ePO-Servers erstellt haben, müssen Sie Folgendes durchführen:

1. Erstellen Sie eine Microsoft SQL Server-Sicherung der Datenbank mithilfe von:
   - Microsoft SQL Server Management Studio
   - Microsoft Transact-SQL
2. Kopieren Sie die erstellte Sicherungsdatei auf den SQL-Wiederherstellungs-Server.
3. Stellen Sie die Sicherung der primären SQL-Datenbank wieder her, in der sich die Snapshot-Datensätze für die Wiederherstellung nach einem Systemausfall befinden. Verwenden Sie dazu:
   - Microsoft SQL Server Management Studio
   - Microsoft Transact-SQL

Ausführliche Informationen über die Durchführung dieser Prozesse finden Sie in der Dokumentation von Microsoft SQL Server.

Dadurch wird ein SQL-Server-Duplikat erstellt, das bei Bedarf wiederhergestellt werden kann. Dazu wird es bei einer Neuinstallation von ePolicy Orchestrator mit der Option **Wiederherstellen** eingebunden.

Server-Einstellungen zur Wiederherstellung nach einem Systemausfall

Wenn Sie einen ePolicy Orchestrator-Server-Snapshot mithilfe der Wiederherstellungsfunktion nach einem Systemausfall erstellen, können Sie den McAfee ePO-Server schnell wiederherstellen.

Konfigurieren von Server-Einstellungen zur Wiederherstellung nach einem Systemausfall

Sie können die bei der Installation von ePolicy Orchestrator verwendete Passphrase für die Schlüsselspeicherverschlüsselung ändern und mit einer SQL-Datenbank verknüpfen, die mit Datensätzen aus dem Snapshot für die Wiederherstellung nach einem Systemausfall wiederhergestellt wurde.

Bevor Sie beginnen

Zum Ändern der Passphrase für die Schlüsselspeicherverschlüsselung sind Administratorrechte erforderlich.



Für Administratoren ist diese Einstellung nützlich, falls sie die während der Installation von ePolicy Orchestrator konfigurierte Passphrase für die Schlüsselspeicherverschlüsselung vergessen oder verlegt haben. Sie können die zuvor konfigurierte Passphrase ändern, ohne diese kennen zu müssen.

Vorgehensweise

Definitionen zu Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

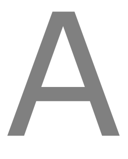
1. Klicken Sie auf **Menü** | **Konfiguration** | **Server-Einstellungen**, wählen Sie in der Liste **Einstellungskategorien** den Eintrag **Wiederherstellung nach Systemausfall** aus, und klicken Sie dann auf **Bearbeiten**.
2. Klicken Sie bei **Passphrase für die Schlüsselspeicherverschlüsselung** auf **Passphrase ändern**. Geben Sie dann die neue Passphrase ein, und bestätigen Sie sie.

   Mit der Passphrase für die Schlüsselspeicherverschlüsselung werden im Server-Snapshot gespeicherte vertrauliche Informationen ver- und entschlüsselt. Sie wird während der Wiederherstellung eines McAfee ePO-Servers benötigt. Notieren Sie sich diese Passphrase.



Die ePolicy Orchestrator-Datenbank muss in regelmäßigen Abständen auf einen Wiederherstellungs-Server der Microsoft SQL-Datenbank kopiert werden, um eine aktuelle Sicherung der Datenbank zu erstellen. Informationen zur Vorgehensweise beim Sichern und Wiederherstellen eines Datenbank-Servers finden Sie unter *Konfigurieren eines Snapshots und einer SQL-Datenbank für Wiederherstellungszwecke*.



Verwalten von ePolicy Orchestrator-Datenbanken

Für eine optimale Leistung und zum Schutz Ihrer Daten müssen Ihre ePolicy Orchestrator-Datenbanken regelmäßig gewartet werden.

Verwenden Sie dazu das entsprechende Microsoft-Verwaltungs-Tool für Ihre jeweilige SQL Server-Version:

SQL Server-Version	Verwaltungs-Tool
SQL Server 2008 und SQL Server 2012	SQL Server Management Studio
SQL Server Express	SQL Server Management Studio Express

Je nach der Ausbringung von ePolicy Orchestrator sollten Sie wöchentlich einige Stunden für reguläre Datenbanksicherungen und Wartungsaufgaben einplanen. Die Aufgaben sollten regelmäßig (entweder wöchentlich oder täglich) ausgeführt werden. Dies sind jedoch nicht die einzigen Wartungsaufgaben, die zur Verfügung stehen. Weitere Informationen zu Wartungsoptionen finden Sie in Ihrer SQL Server-Dokumentation.

Inhalt

Überlegungen zu einem SQL-Wartungsplan

Die SQL-Datenbank ist ein wichtiger Bestandteil von ePolicy Orchestrator. Wenn Sie die in der Datenbank gespeicherten Informationen nicht warten und sichern, können Sie bei einem Systemausfall Ihre gesamte ePolicy Orchestrator-Konfiguration und den Netzwerkschutz verlieren.

Die Wartung der SQL-Datenbank von ePolicy Orchestrator beinhaltet die folgenden beiden Hauptpunkte:

- Wiederherstellung von ePolicy Orchestrator nach einem Systemausfall
- Wartung und Sicherung der SQL-Datenbank

Beide Punkte werden in den folgenden Abschnitten beschrieben.

Wiederherstellung von ePolicy Orchestrator nach einem Systemausfall

Bei der Wiederherstellung von ePolicy Orchestrator wird die Snapshot-Funktion zur Wiederherstellung nach einem Systemausfall genutzt, die in regelmäßigen Abständen die Konfiguration, Erweiterungen, Schlüssel und weitere Elemente von ePolicy Orchestrator in Snapshot-Datensätzen in der ePolicy

Orchestrator-Datenbank speichert. Die in den Datensätzen des Snapshots zur Wiederherstellung nach einem Systemausfall gespeicherten Informationen enthalten die gesamte, zum Zeitpunkt der Snapshot-Erstellung vorliegende ePolicy Orchestrator-Konfiguration.



Damit die Datenbank nach einem Ausfall schnell wiederhergestellt werden kann, ist es wichtig, dass Sie regelmäßig Snapshots Ihrer ePolicy Orchestrator-Datenbank erstellen, die Datenbankdateien sichern und diese Datenbankdatei vom primären SQL-Server auf den SQL-Wiederherstellungs-Server kopieren.

Wartung und Sicherung der SQL-Datenbank

Die SQL-Datenbank ist der zentrale Speicher für alle von ePolicy Orchestrator erstellten und verwendeten Daten. In ihr werden die Eigenschaften der verwalteten Systeme, deren Richtlinieninformationen und Verzeichnisstruktur sowie alle anderen relevanten Daten gespeichert, die der Server benötigt, um Ihre Systeme auf dem aktuellen Stand zu halten. Die Wartung Ihrer SQL-Datenbank in ePolicy Orchestrator sollte daher immer Priorität haben. Die regelmäßigen Wartungsarbeiten an der SQL-Datenbank müssen die folgenden Punkte umfassen:

- Verwaltung von Daten- und (Transaktions-)Protokolldateien. Dazu gehören:
  - Trennen von Daten- und Protokolldateien
  - Korrektes Konfigurieren der automatischen Größenzunahme
  - Konfigurieren sofortiger Dateiinitialisierung
  - Sicherstellen, dass das automatische Verkleinern *nicht* aktiviert ist und dass die Verkleinerung *nicht* zum Wartungsplan gehört
- Indexdefragmentierung. Siehe *Defragmentieren von Tabellendaten*.
- Fehlererkennung. Mithilfe des Tasks zur Überprüfung der Datenbankintegrität oder mittels DBCC CHECKDB.
- Erstellung einer Sicherung und Dateiverwaltung.
- Erstellung eines Plans zur regelmäßigen Ausführung dieser Tasks.

Zum Glück verfügt Ihre SQL-Datenbank über Funktionen (z. B. den Wartungsplanungs-Assistenten und Transact-SQL-Skripte), die Sie so konfigurieren können, dass diese Tasks automatisch durchgeführt werden.

Auswählen eines Modells zur SQL-Datenbankwiederherstellung

Bei ePolicy Orchestrator gibt es zwei Modelle zur Wartung von Microsoft SQL Server-Datenbanken: die *einfache Wiederherstellung* und die *vollständige Wiederherstellung*. Für die ePolicy Orchestrator-Datenbank wird das Modell der einfachen Wiederherstellung empfohlen.

Bei der einfachen Wiederherstellung betrachtet der SQL Server die gesicherten Datensätze als *Inaktiv*, was auch als *Abschneiden* des Protokolls bezeichnet wird. Durch das Abschneiden des Protokolls können nachfolgend protokollierte Vorgänge die inaktiven Einträge im Transaktionsprotokoll überschreiben, wodurch vermieden wird, dass die Protokolldatei zu groß wird.

Bei der vollständigen Wiederherstellung würde das Transaktionsprotokoll so lange anwachsen, bis es schließlich den gesamten freien Speicherplatz auf der Festplatte belegt. Es sei denn, in regelmäßigen Abständen wird eine Sicherung des Transaktionsprotokolls vorgenommen. Wenn Ihre ePolicy Orchestrator-Datenbank so konfiguriert ist, dass sie das Modell der vollständigen Wiederherstellung verwendet, müssen Sie das Transaktionsprotokoll regelmäßig sichern, damit es nicht zu groß wird.

Wenn Sie die einfache Wiederherstellung verwenden, werden die Datensätze bei einem Checkpoint auf die Festplatte ausgelagert, und das Transaktionsprotokoll wird von SQL Server abgeschnitten. Durch dieses Abschneiden wird Speicherplatz in der Transaktionsprotokolldatei frei.

Beim Modell der einfachen Wiederherstellung wird das Transaktionsprotokoll nicht gesichert. Es erfolgen nur die regelmäßigen vollständigen Sicherungen der ePolicy Orchestrator-Datenbank. Nach einem Systemausfall können Sie jedoch nur die letzte vollständige Sicherung wiederherstellen. Alle danach aufgetretenen Änderungen gehen verloren.

Für die meisten Firmenkunden ist das Modell der einfachen Wiederherstellung eine akzeptable Lösung, da größtenteils nur zwischen den Sicherungen protokollierte Ereignisinformationen verloren gehen würden. Wenn Sie das Modell der vollständigen Wiederherstellung verwenden, bringen die regelmäßig durchzuführenden Sicherungen des Transaktionsprotokolls Ihrer ePolicy Orchestrator-Datenbank einen zusätzlichen Verwaltungsaufwand mit sich.

Schon allein aus diesem Grund sollten Sie für die ePolicy Orchestrator-Datenbank die einfache Wiederherstellung vorziehen.

Wenn Sie sich jedoch für die vollständige Wiederherstellung entscheiden, müssen Sie unbedingt sicherstellen, dass Sie sowohl für die ePolicy Orchestrator-Datenbank als auch das Transaktionsprotokoll über einen guten Sicherungsplan verfügen. Erörterungen zu Sicherungsplänen für SQL Server-Datenbanken würden jedoch den Umfang dieses Handbuchs sprengen. Weitere Informationen dazu finden Sie in der Dokumentation von Microsoft SQL Server.

Defragmentieren von Tabellendaten

Einer der wichtigsten Gründe für Leistungsprobleme bei Datenbanken sind defragmentierte Tabellendaten. Zur Lösung dieses Problems können Sie die Tabellendaten neu organisieren oder – falls erforderlich – neu erstellen.

Die Fragmentierung von Tabellendaten in Datenbanken ähnelt dem Index am Ende eines dicken Buches. Ein einzelner Indexeintrag in einem dicken Buch kann auf diverse Seiten im Buch verweisen. Das bedeutet, dass Sie unter jedem einzelnen Verweis nachschlagen müssen, um die gesuchten Informationen zu finden.

Ganz anders bei einem Telefonbuch: Dort sind die Einträge in alphabetischer Reihenfolge sortiert. So kann eine allgemeine Abfrage nach einem Namen wie "Müller" zu einem Suchergebnis führen, das sich über mehrere aufeinanderfolgende Seiten erstreckt, die jedoch immer noch alphabetisch sortiert sind.

Bei einer Datenbank sehen die Tabellendaten anfangs auch wie in einem Telefonbuchverzeichnis aus. Im Laufe der Zeit ähneln sie jedoch immer mehr dem Index eines dicken Buches.

Sie müssen die Daten gelegentlich neu sortieren, um eine Reihenfolge wie in einem gut sortierten Telefonbuch wiederherzustellen. Daher ist es wichtig, dass Sie Ihre Indizes neu organisieren oder neu erstellen. Im Laufe der Zeit nimmt die Fragmentierung einer Datenbank immer mehr zu, insbesondere in größeren Umgebungen, wenn täglich eine Vielzahl von Ereignissen in die Datenbank geschrieben wird.

Damit die Leistung des McAfee ePO-Servers dauerhaft erhalten bleibt, sollten Sie unbedingt einen SQL-Wartungs-Task zur automatischen Neuorganisierung und -erstellung der Indizes erstellen. Sie können die Neuindizierung in Ihren normalen Sicherungsplan einbeziehen, damit alles in einem Task erledigt wird.



Beim Konfigurieren des Tasks dürfen Sie keine Verkleinerung der Datenbank durchführen. Dieser Fehler unterläuft vielen Administratoren beim Erstellen ihres Wartungs-Tasks.

Der Nachteil eines SQL-Wartungs-Tasks besteht darin, dass alle Indizes unabhängig von ihrem Defragmentierungsgrad neu erstellt oder organisiert werden. Damit die Neuerstellung oder Neuorganisierung einer großen Datenbank im Produktionseinsatz möglichst wenig Zeit in Anspruch nimmt, sollten Sie einen SQL Server-Agent-Auftrag konfigurieren, der ein benutzerdefiniertes SQL-Skript ausführt, mit dem Indizes gemäß ihrer Fragmentierung selektiv neu erstellt oder organisiert werden.

Den Fragmentierungsgrad eines Index können Sie ermitteln, indem Sie die dynamische Verwaltungssicht (Dynamic Management View, DMV) **sys.dm_db_index_physical_stats** abfragen. Im Internet sind Informationen zur SQL Server-Datenbankwartung verfügbar, die SQL-Beispielskripte enthalten, mit denen Sie Indizes je nach ihrer Fragmentierung selektiv neu erstellen oder organisieren können. Weitere Informationen dazu finden Sie in der Microsoft-Bibliothek unter sys.dm_db_index_physical_stats (Transact-SQL) im Beispiel D.

Mit folgender Faustregel können Sie feststellen, ob fragmentierte Tabellen neu erstellt oder organisiert werden sollten:

- Weniger als 30 %: Die Tabellendaten sollten neu organisiert werden.
- Mehr als 30 %: Die Tabellendaten sollten neu erstellt werden.



Beim Neuorganisieren des Index – was die empfohlene Option ist – bleibt die Tabelle online, d. h. die Tabelle ist während dieser Zeit für Abfragen verfügbar. Bei stark fragmentierten Tabellen ist eine Neuerstellung möglicherweise die bessere Alternative. Sofern Sie nicht mit SQL Server Enterprise Edition arbeiten, muss dieser Vorgang jedoch offline durchgeführt werden.

Weitere Informationen dazu finden Sie in der Online-Bibliothek von Microsoft unter Neuorganisieren und Neuerstellen von Indizes.

Erstellen eines SQL-Wartungsplans

Erstellen Sie für automatische Sicherungen Ihrer ePolicy Orchestrator-Datenbank einen Wartungsplan für die SQL-Datenbank (z. B. mit SQL Server Management Studio).



Sie sollten die Konfiguration, Erweiterungen, Schlüssel sowie andere Informationen von ePolicy Orchestrator in regelmäßigen Abständen mithilfe der ePolicy Orchestrator-eigenen Snapshot-Funktion in Snapshot-Datensätzen zur Wiederherstellung nach einem Systemausfall in der SQL-Datenbank speichern. Zusammen mit den regelmäßig vorgenommenen Sicherungen Ihrer Datenbank können Sie mit diesen Snapshot-Datensätze Ihren McAfee ePO-Server nach einem Systemausfall schnell wiederherstellen.

Vorgehensweise

1. Erstellen Sie einen neuen Wartungsplan. Informationen dazu finden Sie bei Microsoft unter:
   - Vorgehensweise: Starten des Wartungsplanungs-Assistenten (SQL Server Management Studio)
   - Erstellen eines Wartungsplans

   Der Wartungsplanungs-Assistent wird gestartet.
2. Geben Sie einen Namen für den Wartungsplan ein (z. B. `ePO-Datenbank-Wartungsplan`).
3. Konfigurieren Sie einen Zeitplan für den Wartungsplan. Planen Sie den Task so, dass er außerhalb der Spitzenzeiten ausgeführt wird. Konfigurieren Sie beispielsweise einen regelmäßig ausgeführten Task, der wöchentlich jeden Samstag um 23:00 Uhr ausgeführt wird und kein Enddatum besitzt.

4. Definieren Sie, dass die folgenden Wartungs-Tasks durchgeführt werden sollen:
   - Datenbankintegrität überprüfen
   - Index neu erstellen
   - Datenbank sichern (vollständig)
5. Legen Sie die Reihenfolge für die Wartungs-Tasks wie folgt fest:
   - Datenbankintegrität überprüfen
   - Datenbank sichern (vollständig)
   - Index neu erstellen



Die Reihenfolge dieser Tasks kann geändert werden. McAfee empfiehlt jedoch, die Sicherung der Datenbank vor der Neuerstellung des Index durchzuführen. So wird sichergestellt, dass eine funktionierende Kopie der Datenbank vorhanden ist, falls bei der Index-Neuerstellung ein Problem auftritt.

6. Legen Sie fest, dass der Task "Datenbankintegrität überprüfen" Folgendes umfassen soll:
   - ePolicy Orchestrator-Datenbankname
   - Enthaltene Indizes
7. Legen Sie fest, dass der Task "Datenbank sichern (vollständig)" Folgendes umfassen soll:
   - ePolicy Orchestrator-Datenbankname
   - Pfad zum Speicherort für die Sicherung
8. Legen Sie fest, dass der Task "Index neu erstellen" Folgendes umfassen soll:
   - ePolicy Orchestrator-Datenbankname
   - Objekt: Tabellen und Sichten
   - Prozentsatz für freien Speicherplatz pro Seite ändern in 10 %



Da bei einem Task vom Typ "Index neu erstellen" die Statistik während der Neuerstellung aktualisiert wird (bei vollständigem Scan), ist nach einer Neuerstellung des Index kein Task vom Typ "Statistiken aktualisieren" erforderlich.

9. Legen Sie fest, dass **Berichtsoptionen auswählen** Folgendes umfassen soll:
   - Bericht in eine Textdatei schreiben
   - Nach neuem Ordnerspeicherort suchen

Damit wird ein Wartungsplan zur automatischen Sicherung der ePolicy Orchestrator-Datenbank erstellt.

Ändern der Verbindungsinformationen für SQL Server

Die Konfigurationsdetails für SQL Server-Verbindungen können Sie auf einer speziellen ePolicy Orchestrator-Webseite ändern.

Bearbeiten Sie die Details der Konfiguration einer Verbindung, wenn Sie die Benutzerkontoinformationen in ePolicy Orchestrator ändern oder wenn Sie Änderungen an den SQL Server-Authentifizierungsmodi in SQL Server Enterprise Manager oder SQL Server Management Studio vornehmen müssen. Wenden Sie diese Vorgehensweise an, wenn Sie aus Gründen erhöhter Netzwerksicherheit ein SQL Server-Benutzerkonto mit Berechtigungen benötigen.



Wenn die Datenbankeinstellungen so geändert werden, dass dieser McAfee ePO-Server auf eine McAfee ePO-Datenbank zeigt, die nicht genau übereinstimmt, kann dies dazu führen, dass Produkterweiterungen entfernt werden und alle zugehörigen Daten verloren gehen. Sie sollten diese Aufgabe daher nur durchführen, um die Konfiguration Ihrer vorhandenen Datenbank zu ändern.

Auf der Webseite `https://<Server-Name>:<Port>/core/config` können Sie alle in der Datenbankkonfigurationsdatei enthaltenen Informationen anpassen, die früher mithilfe der Datei `CFGNAIMS.EXE` geändert wurden.

Wissenswertes zu dieser Seite:

- Authentifizierung – Wenn die Datenbank ausgeführt wird, verwendet diese Seite die normale McAfee ePO-Benutzerauthentifizierung, und nur ein Administrator kann darauf zugreifen. Wenn die Datenbank heruntergefahren ist, ist eine Verbindung von dem System erforderlich, auf dem der SQL Server ausgeführt wird.
- Damit Konfigurationsänderungen wirksam werden, muss der McAfee ePO-Server neu gestartet werden.
- Als letzte Möglichkeit könnten Sie die Konfigurationsdatei per Hand bearbeiten (`<ePO-Installationsverzeichnis>server\conf\orion\db.properties`). Geben Sie dazu das Kennwort in Klartext ein, starten Sie den Server, und ändern Sie dann auf der Konfigurationsseite die Datenbankkonfiguration, in der die verschlüsselte Version der Passphrase gespeichert wird.

Vorgehensweise

Definitionen zu Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

1. Melden Sie sich mit den Anmeldeinformationen eines Administrators bei ePolicy Orchestrator an.
2. Geben Sie die folgende URL-Adresse in die Adresszeile Ihres Browsers ein:

   `https://<Server-Name>:<Port>/core/config`

3. Ändern Sie auf der Seite **Datenbankeinstellungen konfigurieren** je nach Bedarf die Anmeldeinformationen oder die SQL Server-Informationen.

   Die anderen Einstellungen auf dieser Seite lauten:

   - **Hostname oder IP-Adresse** – Gibt den Hostnamen oder die IP-Adresse des verwendeten Datenbank-Servers an.
   - **Datenbank-Server-Instanz** – Bei einem Server in einem Cluster wird hier der Name der Server-Instanz angegeben.
   - **Datenbank-Server-Port** – Gibt den Server-Port an, über den die Kommunikation zwischen dem McAfee ePO-Server und dem SQL-Datenbank-Server erfolgt.

- **Datenbankname** – Gibt den spezifischen Namen der auf dem SQL Server verwendeten Datenbank an.
- **SSL-Kommunikation mit Datenbank-Server** – Gibt an, auf welche Weise der Verbindungsport SSL verwendet (**Niemals SSL verwenden**, **SSL verwenden (wenn möglich)**, **Immer SSL verwenden**).

Überprüfen Sie durch Klicken auf **Verbindung testen**, dass die Verbindung zwischen dem McAfee ePO-Server und dem SQL-Datenbank-Server funktioniert.

4. Klicken Sie abschließend auf **Übernehmen**.
5. Starten Sie das System oder die ePolicy Orchestrator-Dienste neu, um die Änderungen zu übernehmen.

B Öffnen einer remoten Konsolenverbindung

Mithilfe des Namens oder der IP-Adresse Ihres McAfee ePO-Servers und dessen Kommunikationsport können Sie von jedem unterstützten Internetbrowser aus eine Verbindung herstellen und ePolicy Orchestrator konfigurieren.



Bei einer remoten Verbindung mit ePolicy Orchestrator sind einige Änderungen an der Konfiguration nicht erlaubt. So dürfen Sie zum Beispiel registrierte ausführbare Dateien nicht über eine Remote-Verbindung ausführen.

Zum Konfigurieren einer Remote-Verbindung müssen Sie den Namen oder die IP-Adresse des McAfee ePO-Servers und dessen Kommunikationsport ermitteln. Notieren Sie sich beim Öffnen von ePO dazu die Adresse, die in Ihrem Browser angezeigt wird, während Sie bei Ihrem physischen McAfee ePO-Server angemeldet sind. Diese sieht wie folgt aus:

`https://win-2k8-epo50:8443/core/orionSplashScreen.do`

Im oben aufgeführten Beispiel haben die einzelnen Bestandteile der URL-Adresse folgende Bedeutung:

- `win-2k8-epo50` – Der Name des McAfee ePO-Servers.
- `:8443` – Die Nummer des Konsolen-Ports zur Anwendungs-Server-Kommunikation, der vom ePolicy Orchestrator-Server verwendet wird.

  Falls Sie diese Nummer nicht geändert haben, lautet der Standardport "8443".

Vorgehensweise

Definitionen zu Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

1. Öffnen Sie einen beliebigen Internetbrowser, der von ePolicy Orchestrator unterstützt wird. Eine Liste der unterstützten Browser finden Sie im *Installationshandbuch von McAfee ePolicy Orchestrator 5.0.0*.
2. Geben Sie im Browser eine der folgenden Zeilen in die Adressleiste ein, und drücken Sie dann die **EINGABETASTE**:

   `https://<Server-Name>:8443`

   `https://<IP-Adresse_des_Servers>:8443`

   Beispiel: `https://win-2k8-epo50:8443`
3. Melden Sie sich bei ePolicy Orchestrator an. Damit ist die remote Konsolenverbindung hergestellt.

Im *Skripthandbuch zu ePolicy Orchestrator 5.0.0* finden Sie ausführlichere Beispiele zu Befehlen, die Sie über eine remote Konsolenverbindung ausführen können.



Häufig gestellte Fragen

In diesem Kapitel finden Sie Antworten auf häufig gestellte Fragen zur ePolicy Orchestrator-Software.

Inhalt

Fragen zur Richtlinienverwaltung

Was ist eine Richtlinie?

Eine Richtlinie ist eine benutzerdefinierte Teilmenge von Produkteinstellungen, die einer Richtlinienkategorie entsprechen. Sie können so viele benannte Richtlinien erstellen, ändern oder löschen, wie es für jede Richtlinienkategorie erforderlich ist.

Was sind die McAfee Default- und die My Default-Richtlinien?

Bei der Installation enthält jede Richtlinienkategorie mindestens zwei Richtlinien. Diese haben die Namen "McAfee Default" und "My Default". Bei Erstinstallationen sind dies die einzigen Richtlinien, die vorhanden sind. Die Konfigurationen sind für beide anfangs identisch.

Die benannten McAfee Default-Richtlinien können weder bearbeitet noch umbenannt oder gelöscht werden. Die Richtlinien vom Typ "My Default" können bearbeitet, umbenannt und gelöscht werden.

Was geschieht mit den untergeordneten Gruppen und Systemen einer Gruppe, der eine neue Richtlinie zugewiesen wird?

Alle untergeordneten Gruppen und Systeme, für die festgelegt ist, dass sie die jeweilige Richtlinienkategorie erben, erben die Richtlinie, die auf eine übergeordnete Gruppe angewendet wird.

Wie wirkt sich die Änderung an einer Richtlinie im Richtlinienkatalog auf die Gruppen und Systeme aus, auf die diese Richtlinie angewendet wird?

Alle Gruppen und Systeme, auf die eine Richtlinie angewendet wird, empfangen an der Richtlinie vorgenommene Änderungen bei der nächsten Agent-zu-Server-Kommunikation. Die Richtlinie wird dann bei jedem Richtlinienerzwingungsintervall erzwungen.

Ich habe eine neue Richtlinie zugewiesen, sie wird aber auf den verwalteten Systemen nicht erzwungen. Warum?

Neue Richtlinienzuweisungen werden erst bei der nächsten Agent-zu-Server-Kommunikation erzwungen.

Ich habe Richtlinienzuweisungen aus einem Quellspeicherort (Gruppe oder System) kopiert und in einem Zielspeicherort eingefügt, aber die im

Zielspeicherort zugewiesenen Richtlinien sind mit denen im Quellspeicherort nicht identisch. Warum nicht?

Beim Kopieren und Einfügen von Richtlinienzuweisungen werden nur echte Zuweisungen eingefügt. Wenn der Quellspeicherort eine Richtlinie geerbt hat, die Sie zum Kopieren ausgewählt haben, wurde im Zielspeicherort nur das Vererbungsmerkmal eingefügt. Daher erbt das Ziel dann die Richtlinie (für die jeweilige Richtlinienkategorie) von dem eigenen übergeordneten Element, sodass es sich um eine andere Richtlinie als die handeln kann, die an den Quellspeicherort vererbt wurde.

Fragen zu Ereignissen und Antworten

Wenn ich eine Antwortregel für Virenfunde erstelle, erhalte ich dann für jedes Ereignis während eines Virenausbruchs eine Benachrichtigung?

Nein. Regeln können so konfiguriert werden, dass eine Benachrichtigung entweder erst beim Auftreten einer bestimmten Anzahl von Ereignissen innerhalb eines bestimmten Zeitraums gesendet wird oder dass höchstens eine Benachrichtigung innerhalb eines definierten Zeitraums gesendet wird.

Kann ich eine Regel erstellen, die Benachrichtigungen für mehrere Empfänger generiert?

Ja. Sie können mehrere E-Mail-Adressen für Empfänger im Assistenten **Antwort-Generator** eingeben.

Kann ich eine Regel erstellen, die mehrere Benachrichtigungstypen generiert?

Ja. Benachrichtigungen für ePolicy Orchestrator unterstützen jede Kombination der folgenden Benachrichtigungsziele für jede Regel:

- E-Mail (einschließlich Standard-SMTP, SMS und Text-Pager)
- SNMP-Server (über SNMP-Traps)
- Externe, auf dem ePolicy Orchestrator-Server installierte Tools
- Probleme
- Geplante Server-Tasks

Index

B

C

D

E

F

G

H

I

J

K

S


McAfee
An Intel Company